Major cyber incident FAQs

Published 15 May 2017
Updated 18 May 2017

Information and technology
for better health and care

FAQs

The purpose of this document is to collate and respond to FAQs received from staff working across the sector to remediate against the ransomware incident on 12 May 2017. This will be an iterative document that will be updated as new questions arise.

What guidance has been issued?

001	Has communications been issued informing trusts the patch will only be successful if servers are rebooted?	Yes. The updated 'Guide to Patching' issued on 14 May via CareCERT and EPRR networks advises: "The machine should install the update and will need to restart. Once the machine has restarted, the patch will be installed." A link to the guidance is here https://www.digital.nhs.uk/media/1483/Patch-guidance-140517/pdf/Patch_guidance_1405173
002	What are the latest recommendations on applying patching and antivirus updates?	A follow-on bulletin on 'Guide to Patching' was distributed via CareCERT and EPRR networks on 14 May which will provide updated recommendations and more detailed guidance on how to apply patches to your organisation's operating system.https://www.digital.nhs.uk/media/1483/Patch-guidance-140517/pdf/Patch_guidance_1405173
003	Do you have any advice on blocking ports - additional updates or recommendations about which websites or IP addresses to block?	The CareCERT bulletin distributed on 14 May covers this issue in greater detail. WannaCry Ransomware Using SMB Vulnerability (CC-1411)
004	How can we ensure updates from radiology vendors and medical vendors with regards to antivirus updates for their machines?	NHS Digital wrote to all system suppliers on 14 May to request they treat this incident with the highest priority and do everything they could to support their NHS customers by engaging with them directly.

		Please contact your radiology or medical vendors directly to get confirmation that they have applied the latest AV files to your machines. We continue to work with NHS England and others to identify and support specific cases as needed.
005	Many technology suppliers maintain their own systems and we are not always aware of how these suppliers update them. Are there plans for a national conversation with main NHS providers and advice to the NHS?	NHS Digital wrote to all system suppliers on 14 May to request they treat this incident with the highest priority and do everything within their capability to support their NHS customers at this time by engaging with them directly. We continue to work with NHS England and others to identify and support specific cases as needed.
006	How do I keep up-to-date with latest developments on the vulnerability and the malware? Where is NHS Digital and CareCERT publishing this?	CareCERT will continue to distribute regular alerts regrading this. However for the most up-to-date information, the Information Sharing Portal article is regularly updated: https://nww.carecertisp.digital.nhs.uk

Is it safe for me to use my PC?

007	Is it safe for me to turn on my PC when I arrive in the morning?	We would recommend that you check this with whoever is responsible for IT updates within your organisation. Technical guidance is to turn on systems whilst in a quarantined state and look for signs of infection. If no infection is present, apply the patch and reconnect to network. If infection is present, re-image, apply patch and reconnect to network.
008	Is there a risk that devices that have been switched off for a few days could cause a second phase of reinfection when they are switched on again?	We are not aware that further waves are planned. The patching of systems removes the vulnerability that the ransomware exploits. NHSmail and the gateways to the Transition network (N3) are working to ensure central systems can spot malicious activity. If this situation changes sites will be notified via CareCERT and the NHS England EPRR leads.

How do I use the patch?

009	What happens if I apply the patch but I find the	Applying the patch will not fix encrypted files. You will need to roll back infected

	files are still encrypted?	machines and apply the patch to those machines. This should be done by your local IT support team.
010	Once I have applied the patch, can I reconnect to N3?	Yes, as long as the patch has been applied across your estate. You should have disconnected Infected computers from the network immediately, and before applying any patches. The machine should be re-imaged and built from a known good back-up before being entered back on to a clean network or before any centralised deployment methods are utilised. These activities should be carried out by your local IT support team.
011	If my site is unaffected but we have applied the patch, do we still need to roll back?	No, if your site is not infected and the patch is applied then there is no need to roll back.
Primary care		
012	What is being done for GP practices that may have infected files?	The initial focus has been on containing the threat to urgent care services. The focus then moved towards ensuring primary care services are appropriately patched to reduce risk. All CSUs across the country are engaged through NHS England to ensure GP practices within their regions are patched. Communications went out to all GP practices on 15 May on how to apply the patch and there is further guidance on the NHS Digital Website
Are NHSmail and N3 affected by this attack?		
013	My site is unaffected, do I need to disconnect from N3?	There is no evidence to suggest N3 or NHSmail have been compromised. Unaffected and fully patched sites can remain connected to these national systems. However, it is important to have an efficient patching regime and continue to action CareCERT advice.
014	Can the timeout on the NHS relay server be extended? Most trusts turn external mail as they patch. The 48-hour limit will mean emails are bounced tomorrow; adding an additional 24	The re-try limit on the Gateway was increased from 48 hours to 72 hours on Saturday 13 May at the request of our partners. This means organisations that switched off their N3 links will avoid large volumes of non-delivery receipts (NDRs). This extended re-try period has now expired for those organisations

	hours would help.	that switched off their connection on Friday 12 May. Once connection has been re-established, users will receive NDRs for the messages that were sent just before, or during the switch-off period. Local Administrators should remind their users that if any emails were sent during this time, they will need to re-send them.
015	Can you confirm, where possible, that no emails have passed through the NHSmail Email Gateway or Exchange solution with the attachments we're currently aware of?	Since we started to see the impact of the Wannacry ransomware attack on Friday, NHS Digital and Accenture have been investigating the NHSmail platform to determine whether it was used in the attack, or compromised as a result of the attack. Following rigorous investigation, NHS Digital can confirm that the platform has not been compromised, nor has it been used as a delivery mechanism for the ransomware to infect or spread. Organisations who have removed their access to NHSmail, given the above reassurances and checks carried out, should now start to seriously consider re-enabling access to NHSmail services.
What are the known facts about this attack?		
016	Is the current ransomware likely to mutate or are there any other variants?	It is possible that the ransomware could be repurposed to exploit a different vulnerability or render the kill switch inoperable. It is currently unclear whether the attacker has any mechanism to remotely update this malware or download files or if there is a backdoor though this is unlikely. Deploying the Microsoft patch should help defend against this and any variants. We advise further mitigation as per previous guidance released by the National Cyber Security Centre and NHS Digital.
017	We believe that the attack began from a compressed Zip file. Can you confirm that its method of entry is now clear?	This has not yet been confirmed. Investigations into the attack vector continue but have uncovered no indication NHSmail has been compromised or is the method of attack.

		NHSmail has several levels of filtering in place, including safe testing of suspicious files. Any emails with known bad URLs or IP addresses are also filtered out at site.
Guidance for home users and small businesses		
018	I work for a very small organisation and we do not have a local IT helpdesk, is there any guidance I can follow to ensure my PC is protected?	The NCSC has published guidance for home users and small businesses on 14 May: https://www.ncsc.gov.uk/guidance/ransomware-guidance-home-users. The patching guidance will support you in ensuring your systems are protected.

Further Support

For the guide on applying the Microsoft patch referred to in FAQs above, please see:
https://www.digital.nhs.uk/media/1483/Patch-guidance-140517/pdf/Patch_guidance_1405173

For information about this specific incident and detailed technical remediation advice, please see:

WannaCry Ransomware Using SMB Vulnerability (CC-1411)

All threat broadcast and guidance can be found here:

https://nww.carecertisp.digital.nhs.uk

To understand more about ransomware and how to protect your organisation, please see this article on the CareCERT Information Sharing Portal:

https://nww.carecertisp.digital.nhs.uk/display/CC/Ransomware+-+Preparing+for+an+Outbreak

If you don’t have access to Transition Network (N3), refer to the latest NCSC guidance on ransomware:

https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance

https://www.ncsc.gov.uk/guidance/ransomware-guidance-home-users