NHS Wannacry Ransomware Attack - Is it safe to connect to NHSmail?

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.

Checks have been completed in the following areas:

Email Gateway

- There is no evidence to suggest that NHSmail has been compromised in any way - all analysis has been sent to our Gateway provider.

Exchange

- All mailboxes across the platform continue to be actively checked, scanned and monitored with no discovery as yet of any malware.

Patching

- All core supporting servers are patched in line with Microsoft's latest guidance.

Firewall IP Address Blocking

- All known IP addresses provided by our security colleagues have been blocked across our firewalls that protect the service

Relay Timeout

- Additionally, the re-try limit on the Gateway was increased from 48 hours to 72 hours at the request of our partners. This means organisations that switched off their N3 links will avoid large volumes of NDRs.

This extended re-try period has now expired for those organisations that switched off their connection on Friday 12 May. Once connection has been re-established, users will receive non-delivery receipts (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.

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.

Several documents have been distributed today and these are now available to access on the Information Sharing Portal. These are:

Cyber Incident FAQs
Simple advice on patching individual machines
NHSmail cyber security guide

NHS Digital – Latest guidance for NHS on protecting against cyber attack