**The key components of the incident response of the WannaCry Ransomware Attack**

1. Identification of the vulnerability exploited (SMB v1)
2. Pathing infected systems
3. Implementing network segmentation to prevent further spread
4. Data recovery
5. Investigating the attack to understand its scope and potential effect.
6. Talk with affected users and the way we are solving this problem.
7. Malware scanning
8. Updating all systems
9. Run the latest virus scan
10. Path all systems where its needed

**Stated on Wikipedia Web-Site**

**--------------------------------------------**

The effects of the attack also had political implications; in the [United Kingdom](https://en.wikipedia.org/wiki/United_Kingdom), the impact on the [National Health Service](https://en.wikipedia.org/wiki/National_Health_Service) quickly became political, with claims that the effects were exacerbated by government underfunding of the NHS; in particular, the NHS ceased its paid Custom Support arrangement to continue receiving support for unsupported Microsoft software used within the organization, including Windows XP.

**What was the response from this ransomware attack**

**-----------------------------------------------------------------------------**

Immediately disable automatic tasks., deleting temporary files or rotating logs on the affected systems.

Try to isolate all the infected systems, you don’t want it to spread to other systems. Turn off bluetooth and all of your storage devices until they could be scanned. Then you can start to putting the systems back online.

**----------------------------------------------------------------------------------------------------------------------------------------**

**By**: Thomas Kolenda **Date:** 10/28/2024