**Activity 2**

The WannaCry Ransomware attack that occurred in May 2017 was focused towards Microsoft globally. As such, millions of systems were infected because of a leaked Windows vulnerability. It was carried out in a peculiar way, as a month after a Windows patch had updated, hackers had discovered the vulnerability in the previous version of said patch. WannaCry was a worm, and it was used for the delivery. As worms do WannaCry was able to duplicate itself across the entire network the devices were on, infecting it. Windows was not able to act in time for the patches; the systems that had not been updated were all infected. If Windows was aware of the vulnerability and patched it, they must have been more prominent about how severe it was needed.

Without the software update there wouldn’t have been much to do. The best course of action would be to keep one’s system secure by encrypting it. Encrypting any device would have prevented it from being attacked. Also be reminded that suspicious emails should remain unopened, as well as taking special care not to open links from any untrusted website. Other ways would have been to have booted with a different operating system.

References

<https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/#:~:text=Many%20local%20organisations%20could%20not,Chief%20Executive%20Officers%20by%20telephone>.

<https://www.kaspersky.com/resource-center/threats/ransomware-wannacry>