CYBERSECURITY COMMUNICATION
Please circulate

May 12, 2017

To: University Cybersecurity Communication Recipients
From: University Systems
RE: New Ransomware Variant - WannaCry

University Systems has been monitoring the ransomware attack targeting the National Health Service in the U.K. The operations of the NHS has been disrupted by the outbreak of a significant ransomware attack that is spreading across organizations globally.

This new ransomware variant known as “WannaCry” appears to be spreading through a vulnerability in Windows that was patched on March 14, 2017 and vulnerabilities in Office that were patched on May 9, 2017. Details on these critical security update from Microsoft are available in the following Microsoft bulletins:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/bc365363-f51e-e711-80da-000d3a32fc99

We recommend that you verify that Windows workstations and servers in your area have applied the Microsoft Updates for this issue to mitigate the risk of this ransomware. Servers running Windows Server 2003 are vulnerable and there is no patch available; these should be removed from the network or have TCP port 445 blocked.

If you have any questions about this issue or recommendations, please reply to this message.

Regards,

Marcus

Marcus Greenshields
Cybersecurity Working Group
University Systems
University of Victoria

University of Victoria

To verify the authenticity of this message, visit:
www.uvic.ca/systems/verify