WannaCry Ransomware

Section 16, Lecture 52

**Safeguard your computers or enterprise systems from WannaCry**

**What should you do?**

1.Ensure DeepGuard and real-time protection is turned on in all your corporate endpoints.  
  
2.Identify endpoints without the Microsoft issued patch (4013389) with Software Updater or other available tool.  
  
    
3**.**Patch it immediately with Software Updater or other available tools.

In case you are unable to patch it immediately, we recommend to disable SMBv1 with the steps documented at **Microsoft Knowledge Base Article 2696547** in order to reduce attack surface  
  
  
4.**Configure the firewall to properly block traffic**

Block 445 inbound to all internal and internet-facing Windows systems to prevent workstations from getting infected

Block 445 outbound from servers to prevent the servers from spreading WannaCrypt within the environment

Alternatively, you can set F-Secure Firewall policy to its highest  
setting, which has predefined rules to block the attack. (Recommended)