WannaCry FAQS

Rev Date: 02 May 2022

1. **Does Keysight offer general guidance on how to protect Keysight instruments from infection by computer viruses?**
   Yes. Keysight's Computer Virus Control Program, available here, contains recommendations and guidance.

2. **What Keysight products are vulnerable to the WannaCry virus?**
   Any Keysight product based on the Windows XP, 7 or 10 operating system is potentially vulnerable.

3. **How do I know if my Keysight instrument is infected?**
   You will see something like the following image:

4. **Is there a way to detect if my Keysight instrument is infected prior to the virus fully encrypting the instrument?**
   Once the virus hits a device, it's likely that it will start infecting right away. However, it takes some time to encrypt all the files on the device. High CPU utilization *__may__* be an indicator that the device is in the process of being encrypted. The malware creates files with the suffix ***wncry*** during the encryption process. If the users find any of these files they should immediately remove the device from the network.

5. **What should I do if I have an infected Keysight instrument?**
   Keysight recommends that you contact the local Keysight Business Center to get started. Keysight SSG

has developed service numbers and pricing for repair. In some cases, a recalibration will be required. For instruments, still under warranty, this will be treated as a warranty repair.

6. **Is there a cost to repair my Keysight instrument?**
   Keysight SSG has developed service numbers and pricing. If the instrument is under warranty, it will be considered a warranty cost.

7. **What steps can I take now to protect my Keysight instruments?**
   We encourage all customers with Windows-based instruments to review the Microsoft customer guidance for WannaCry attacks at https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ and ensure their instruments have the latest critical security patches installed.

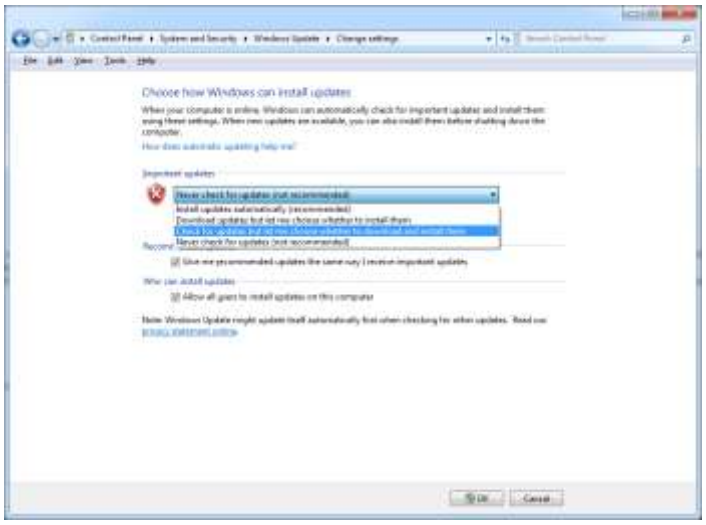
   Other References:

   - Microsoft Security Bulletin MS17-010: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
   - Microsoft KB4012598 Update Catalog for legacy OSs: http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
   - SANS (indicators): https://isc.sans.edu/forums/diary/Massive+wave+of+ransomware+ongoing/22412/
   - Technical description of WannaCrypt:
     - https://www.us-cert.gov/ncas/alerts/TA17-132A
     - https://isc.sans.edu/diary/22420
     - https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

8. **I installed the security patch and now the Keysight instrument isn't working. What should I do?**
   There are no confirmed reports that installing the security patch affects instrument operation. If you encounter such an instance, contact the local Keysight Business Center.

9. **What else can I do to protect my Keysight instruments from a virus or malware?**
   Keysight recommends customers enable automatic update notifications so that as other critical security patches become available they will be notified and they can make a choice to accept or not. In some cases, such as production areas, it may not make sense to enable such notifications, but that is a business decision the customer should make, considering their specific risks. Instructions from Microsoft can be found here. A Windows 7 example is below - via "Change settings" under Windows Update, select "Check for updates but let me choose whether to download and install them."

WannaCry FAQS



Additional information can be found in Keysight's Anti-Virus Policy and Program documents:

- ***Policy***
  http://about.keysight.com/en/quality/Keysight_Computer_Virus_Control_Policy.pdf
- ***Program***
  http://about.keysight.com/en/quality/Keysight_Computer_Virus_Control_Program.pdf

10. **Should I run anti-virus scans on my Keysight instruments?**
    See the FAQ in the Keysight Program document here.

11. **What if I am still running a Keysight instrument on XP?**
    Microsoft has issued a patch that can be found here. Customers will need to have Service Pack 3 installed - see this link.