KEYSIGHT TECHNOLOGIES

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, California 95403

www.keysight.com

Effective: 1 August 2014

Keysight Technologies Computer Virus Control Program

Keysight Technologies, Inc. recognizes the potential risk of computer virus infection that may be posed by instruments which are capable of connecting to computers or networks. We take this threat seriously and have acted to minimize the threat. The following Frequently Asked Questions (FAQ) address key areas of concern.

1. What steps do you take to protect your instruments from infection by computer viruses?

a. Keysight has enacted a number of measures to take all reasonable precautions to prevent the spread of viruses from instruments to our customers' computers and networks. In addition to implementation of centrally managed firewall and anti-virus (AV) programs for all business computers, all computers used in operations that touch instruments destined for customers maintain the latest virus definitions and are scanned regularly.

b. Strict virus control protocols have been enacted in manufacturing, service, support, sales, distribution and demonstration environments. These include the use of isolated LANs, control of removable memory devices, scanning of instruments and removable memory devices and/or reimaging hard drives, as appropriate depending upon instrument configuration.

c. Keysight-wide training of all personnel who come in contact with customer instruments to reinforce anti-virus security protocols. These employees include manufacturing, service, support, sales, distribution and demonstration equipment management personnel.

2. How does Keysight respond to reports of viruses on their instruments?

a. All reports of potential instrument infections are escalated to the General Manager of Quality and Customer Experience, in the same way any safety related incident that poses a threat to a customer's personnel or property would be reported. In the event a customer reports an infection OR Keysight reports that an instrument is infected upon receipt (for service, or from demonstration), the following steps occur:

   i. Immediate Mitigation/Vector Control – Keysight works with the customer to mitigate the threat, by either taking the unit back and replacing it with a clean instrument, or working with the customer to scan and eliminate the viral threat.

   ii. Trace source and extent of the infection to understand where and when the virus was introduced, the nature of the virus and potential for damage. Where appropriate, a thorough report of findings is presented with recommendations for corrective actions to prevent the future spread of viruses.

   iii. Once the threat is thoroughly understood and the infection vectors are determined, internal preventative actions are updated to adjust to the new threat(s). If it is determined that the virus originated outside of Keysight, Keysight will recommend actions to protect our customers' instruments.

3. What can I do to protect my instruments from viruses?

a. As with personal and business computers, the user must take appropriate steps to protect their instruments from infection. This may include installing the latest operating system security patches, installing and running anti-virus software, use of strong firewall settings, eliminating the use of detachable memory devices (e.g., USB thumb drives, portable hard disks), and regular scanning of any memory device used with an Keysight instrument. While Keysight does NOT recommend running anti-virus software in the background on Windows®[i] based instruments due to potentially degrading performance, it does recommend installation of anti-virus software and running it during non-critical hours at least once per week.

4. Where can I learn more about my instrument, how it is configured and how to protect it?

a. Keysight offers more than 600 models of instruments to our customers, with tens of thousands of possible option combinations and configurations. With respect to those attributes that make instruments potentially vulnerable to computer viruses, our instruments may contain any combination of hard disk and solid state memory, USB and LAN ports for both general purpose and proprietary communications, and Windows and non-Windows operating systems of various vintages. With the variety of possible configurations, it is impractical to list details for each and every configuration. In order to help our customers understand potential virus control measures, we classify our instruments into the following categories:

Category 1: A Windows XP/Vista/7 based machine.
Description: PC based instrument running Windows XP, VISTA or 7, or Windows Embedded operating system.
Characteristics: Typically behaves the same as a desktop PC, with ability to connect to LAN, USB devices, keyboard, external monitor, etc. Typically boots from an internal hard disk drive. Are susceptible to current generation of wild viruses, which may either reside or execute on the instrument.

Recommendation:

- Install customer preferred anti-virus scanning (AVS) software, scan regularly. Not recommended to run AVS in background mode as it will impact instrument performance.
- Instrument may also be mounted as a disk drive on a network and scanned from another PC.
- Deactivate Autorun.inf to prevent inadvertent execution of malicious code on portable memory devices.
- Enable strong firewall settings.

Category 2: A Windows98/2000/CE based machine
Description: PC based instrument running Windows 98, 2000 or CE or Windows Embedded operating system.
Characteristics: Typically behaves the same as a desktop or handheld PC; may have ability to connect to LAN, USB devices, keyboard, external monitor, etc. Typically boots from an internal hard disk drive or solid state memory. May be susceptible to current generation of wild viruses, but less likely than current generation OS. Viruses may either reside or execute on the instrument.

Recommendation:

- Due to age, Anti-virus software and current definitions may not be available...
- Instrument may be mounted as a disk drive on a network or over USB and scanned from another PC.
- Deactivate Autorun.inf to prevent inadvertent execution of malicious code on portable memory devices.
- Enable strong firewall settings.

Category 3: A non-Windows machine that can share files and can be mounted as a drive.
Description: PC based instrument running non-Windows operating systems such as LINUX, UNIX, VxWorks, etc.
Characteristics: Special purpose computing engine and operating system optimized for specific task. May have LAN connectivity. May have USB connection for data transfer, license and firmware uploads. Not susceptible to current generation wild viruses but may harbor viruses and pass to host computer.

Recommendation:

- Instrument may be mounted as a disk drive on a network or over USB and scanned from another PC.

Category 4: A non-Windows machine that can share files but can't be mounted as a drive.
Description: Microprocessor controlled instrument running proprietary firmware or non-Windows operating systems such as LINUX, UNIX, VxWorks, etc.
Characteristics: Special purpose computing engine and operating system optimized for specific task. May have LAN connectivity. May have USB connection for data transfer, license and firmware uploads. Cannot be mounted as a disk drive on a network, LAN communications may only allow instrument control and data transfers. Not susceptible to current generation wild viruses but may harbor viruses and pass to host computer.

Recommendation:

- Virus files would have to be copied intentionally to these types of instruments, scanning would require copying files to removable memory device and scanning resultant image.

Guidelines for Installing and Running Antivirus Software on PC based Instruments

NOTE: While Keysight recommends periodically running anti-virus software on Windows operating systems based instruments and scanning non-Windows based instruments, it does not endorse or recommend specific anti-virus software. It is up to the consumer to evaluate and select an anti-virus product which best suits their needs.

The instructions given below are intended to provide a generic process to guide customers through a typical process. Always read and follow the instructions provided by your anti-virus software vendor.

- Close all applications on the instrument so you are left with only Windows running.
- Install anti-virus software per vendor instructions.
- Reboot the instrument – some AV software requires a reboot, Keysight recommends rebooting for all installations.
- Install any virus definition updates available
- Run virus scan software.
    - Allow AV software to quarantine or erase any malware found during the scan
    - If any analysis of viruses is required, follow AV software vendor directions. Keysight is not set up nor has the expertise to evaluate computer viruses.
- When scan is completed, follow AV software vendor's directions for disposing of viruses.
- Close Anti-virus software.

NOTE: Keysight does not recommend routinely running anti-virus software in the background while instruments are in use, as there may be an impact on instrument performance. Depending upon your anti-virus vendor's licensing terms, you may be required to remove the anti-virus software before deployment. If so, please follow anti-virus vendor's procedure for uninstalling.

Special Note Concerning Windows CE Based Products

Based on current information, Windows CE has not become a wide spread target for viruses, worms or malware, and programs written for non-CE based Windows operating systems (i.e., Win98, Win2000, Win XP, Vista, etc.) will not run on Win CE based instruments. But, it is possible for a Win CE devices to transfer a file between two Windows based machines either through direct connect or via a network connection. As a result, Keysight strongly recommends that all Windows based computers that may connect to a Windows CE Embedded device utilize the most current versions of anti-virus software available. Further, Windows CE virus scanners are available, but have not been tested by Keysight.

Guidelines for Scanning Non-Windows Based Instruments

Many non-Windows based instruments may be addressed as a mountable drive by Windows based PCs for the purpose of uploading and downloading data. As such, these instruments can potentially become infected by computer viruses if they are in contact with an infected PC or instrument. As a result, Keysight recommends periodically scanning non-Windows based instruments for viruses to maintain a secure computing environment. Keysight recommends using a PC or Windows based instrument that is capable of communicating with the instrument of interest over LAN or USB.

- Determine if the instrument is recognized as a removable memory device by the host computer.
- If the PC or Instrument recognizes the newly connected instrument AND assigns it a drive letter, it has been recognized, and is ready for scanning.
    - If the Host does NOT recognize the instrument, then using information based in the manual determine if it should be recognizable. If not, then the instrument should not pose a threat to a Windows based PC, instrument or network.
- Scan the instrument as a removable drive using Anti-virus vendor's procedures.
    - For example:
        - Open "My Computer"
        - Locate the Instrument in the list
        - Right click on the instrument, select "Scan for Viruses" from the list

  - Allow virus scan to complete
  - Dispose of viruses per vendor’s recommendations
- Close Anti-virus software
- Disconnect scanned instrument.

Keysight does not recommend running a virus scan while instruments are in use. Periodic scans using updated virus definitions are recommended.

[i] Windows and MS Windows are U.S. registered trademarks of Microsoft Corporation.