SECURITY BULLETIN

Kodak DirectView PACS SYSTEMS 4 and 5 - New Mydoom/Novarg Virus

1.0 Overview

This bulletin addresses a potential threat in most Windows-based systems that use *Microsoft Outlook, Outlook Express* or a web-based e-mail client. The "Mydoom" or "Novarg" virus is classified as a worm. The virus, and its older variants, e.g., W32/Sobig, W32/Swen@mm, can be encapsulated in an e-mail attachment, which upon opening can install malicious code on the system. The worm then propagates itself by sending a message to the contacts in the user's e-mail Address Book. This virus is also reported to have the ability to participate in a "Distributed Denial Of Service Attack" (DDOS Attack), which might prevent access to websites, including the *Microsoft* website.

2.0 Scope

1) Dedicated Systems: Since AutoRad, DirectView CX/DX Workstations (versions 4.x and 5.x), StudyServers, DirectView Workgroup Servers, DICOM Servers, ClinicalAccess / DirectView TX Servers and DMI Web servers are not to be configured for use with any e-mail client; **this virus should not affect them.**
2) Personal Systems: ClinicalAccess and DirectView TX clients, as well as DirectView Web and DMI Web clients installed on personal Windows-based workstations that are also used for e-mail **ARE considered vulnerable.**

3.0 Action

No action is required for properly configured, Dedicated Systems as defined in 1) above.

Customers and users of Personal Systems as defined in 2) above should read below. Customers who apply Security Updates to these Personal Systems do so at their own risk and are solely responsible for the outcome. Kodak Service is not responsible for these systems.

In general, Kodak makes certain recommendations to our customers that enable them to protect the integrity of their network. Some of these recommendations include:

- Customers should maintain a secure network; by implementing third-party firewalls and anti-virus software, which can prevent malicious attacks and infection.
- Any defense mechanisms utilized, must be kept up-to-date.
- Use caution when opening e-mail attachments and downloaded applications.

For Personal Systems with e-mail clients, in the event an infection does occur, please contact your Systems Administrator.

The following links contain additional information provided by third-party vendors who specialize in the prevention and removal of malicious code. This is provided for informational purposes only, and does not constitute any endorsement of these vendors or their products.

http://www.microsoft.com/security/antivirus/mydoom.asp

http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.html

http://vil.nai.com/vil/content/v_100983.htm