

Deloder worm loads VNC and its password, watch out...

by Kyle Lai, KLC Consulting, Inc. --- March 27, 2003

KLC Consulting has confirmed that the Deloder worm is resurfacing. It is again hitting the Windows 2000 and XP systems that are on cable modem and DSL high-speed Internet connections worldwide. Many home users are still un-aware of the problems because they only hit home computers that are on home networks, and many home users haven't got home networks. If the Deloder worm infects a system, anyone with malicious intent (hackers) will be able to use free remote control software (VNC) to connect to that infected system. Once hackers use VNC with the correct password, they can eventually view the computer screen and take over the keyboard and mouse control, just as if they were sitting in front of the infected systems. Deloder worm is classified as a backdoor type of worm, and people who have their computers compromised with these types of worms/Trojans should not expect any privacy unless they totally remove these worm/Trojans.

KLC Consulting did a follow-up experiment (original experiment is at http://www.klcconsulting.net/deloder_worm.htm). A computer was put online from 11PM, 3/25/2003 to 4AM, 3/26/2003, to see if any Deloder worm related activities could be caught from both the US and East Asia, where people have the worst Deloder worm activities. There were 13 Deloder like (Port 445 connection) attempts during this period of time. These source computers were scanned, and of the 13, 10 had evidence of a VNC server component running (TCP port 5800 and 5900 open).

These infected computers can be connected to and remote-controlled using VNC client with password "strict", the default password set by the Deloder worm. There are still incredible numbers of small business and home PC's out there that are vulnerable due to the lack of security awareness and weak passwords, which Deloder type worms took advantage of. Many Deloder worm victims don't realize they are infected because users can still get online and the computer still functions normally. This is especially true when high-speed Internet connections are used with only one computer online at a time. What they don't know is that someone could be watching their screen and spying their every keystroke and mouse movement.

As mentioned earlier, as the result of the Deloder infection, anyone with malicious intent can connect to infected systems and remote control, steal private information, or spy every move on the screen via VNC client at any time. In addition, there is no obvious indication of any VNC activities unless the system owners use netstat (comes with Windows 2000 & XP) or any other TCP/IP port viewer to show connection status.

None of the Anti-Virus vendors' analyses mention the registry key that contains the settings of the VNC server component of Deloder, but indeed it included the password that was set by the Deloder worm, "strict". KLC has notified CERT about the of the problem because the infected systems now all have the same password, waiting for anyone to connect.

In order to properly secure compromised systems, these systems must run anti-virus scans, as well as anti-Trojan scans, and install personal firewalls. KLC has updated the Deloder analysis, and is available at http://www.klcconsulting.net/deloder_worm.htm, where it has recommendations for securing compromised system and protecting systems from future incidents.

KLC Consulting is committed to protecting the availability, confidentiality, and integrity of the information and data assets of our clients. KLC has qualified security engineers that will help you design, build, and achieve balanced security solutions base on your business objectives.