FOR IMMEDIATE RELEASE 25-9-08          Contact: Craig Rowe (07) 3883 3550

# ROGUE SOFTWARE WREAKS HAVOC

Many people have commonly heard terms like computer virus and spyware, however in recent years a new breed of malicious software has been wreaking havoc on people's computers.

These applications are known as rogue malware designed to fool users into believing they are infected with a virus.

RSU Computer Solutions proprietor Craig Rowe said his business had fixed several computers infected with a rogue application known as 'XP Antivirus' in recent weeks.

"By all appearances the software seems to be legitimate, but the application is in fact a malicious program which takes control or hi-jacks key features of the operating system and reports false readings of virus infection to the user," he said.

"Last week we removed a new variant of the software called 'XP Antivirus 2009' which has been circulating the internet since July this year."

Mr Rowe said the antivirus software companies are behind the eight ball as the cyber criminals continue to evolve their applications to avoid detection.

He said, "It's an ongoing battle between them."

"People may ask why anyone would bother writing such harmful applications."

He said the authors of 'XP Antivirus 2008/09' actually wanted people to purchase a full copy of their software to remove the infection which was caused by them in the first place.

To avoid infection RSU Computer Solutions recommends people keep their virus scanning and anti-spyware software up to date and scan their computer regularly.

If you encounter the rogue software and have trouble removing it or any other computer virus RSU provides an on-site pc repair service.

For more information phone (07) 3883 3550 or visit www.rsu.com.au

# Harmful Program Definitions *by RSU Computer Solutions*

**Virus:** A program which infects files in order to spread itself, it may corrupt data or deliver some other payload causing data loss or damage to the host computer.

**Trojan:** A Trojan is not a virus itself but a file that appears harmless. When run, a trojan may cause harm to computer data, system performance or network speed. A Trojan's payload may be capable of almost any type of harm.

**Worm:** A worm spreads itself to other computers without needing to be transferred from a host. In general, a worm does not actually harm either the system's hardware or software, it simply executes itself and moves on, but spreads rapidly resulting in reduced network performance. It may use a persons email contact list to forward itself on.

**Hi-Jack:** An application which takes control of key features of an operating system, commonly Internet Explorer and key security features like System Restore and the System Registry. It is common for buttons to be added to Internet Explorer and for users to be locked out of changing the desktop. Internet Explorer may constantly redirect search engine results to harmful websites normally containing rogue malware.

**Rogue Malware:** Software which looks legitimate, but is downloaded by deception and gives false reports of virus infection. It often includes hi-jack techniques to annoy the user into purchasing a full copy of the fake application.

**Spyware:** Programs that Install and gather information from a computer without permission, and report the information to the creator of the software or to one or more third parties.

**Adware:** The difference between Adware and Spyware is very subtle. Both Adware and Spyware are installed without the user's permission on a machine. An Adware's main purpose is to display targeted ads based on the user behaviour it is tracking.

**PUP (Potentially Unwanted Program):** A program that is legitimate, but has some questionable methods of obtaining data or information from the user.

**Downloaders, Tricklers & Dialers:** While many are legitimate and are included as update features of many applications, some Trojans may actually install these small programs which download rogue software in the background without users knowing. Once downloaded the payload is delivered with often harmful consequences.

**Phishing:** Fraudulent e-mail or website claiming to be legitimate seeking identifiable information. Phishing is an attempt to steal your personal data including user names and passwords to bank accounts, credit card details and social security or tax information. It is one of the biggest internet threats at present resulting in identity theft.

**Malicious Script**: Malicious scripts may run as part of your browser and could download and install software on your computer and can also be used to alter the appearance of the browser, thus making phishing attacks more successful.
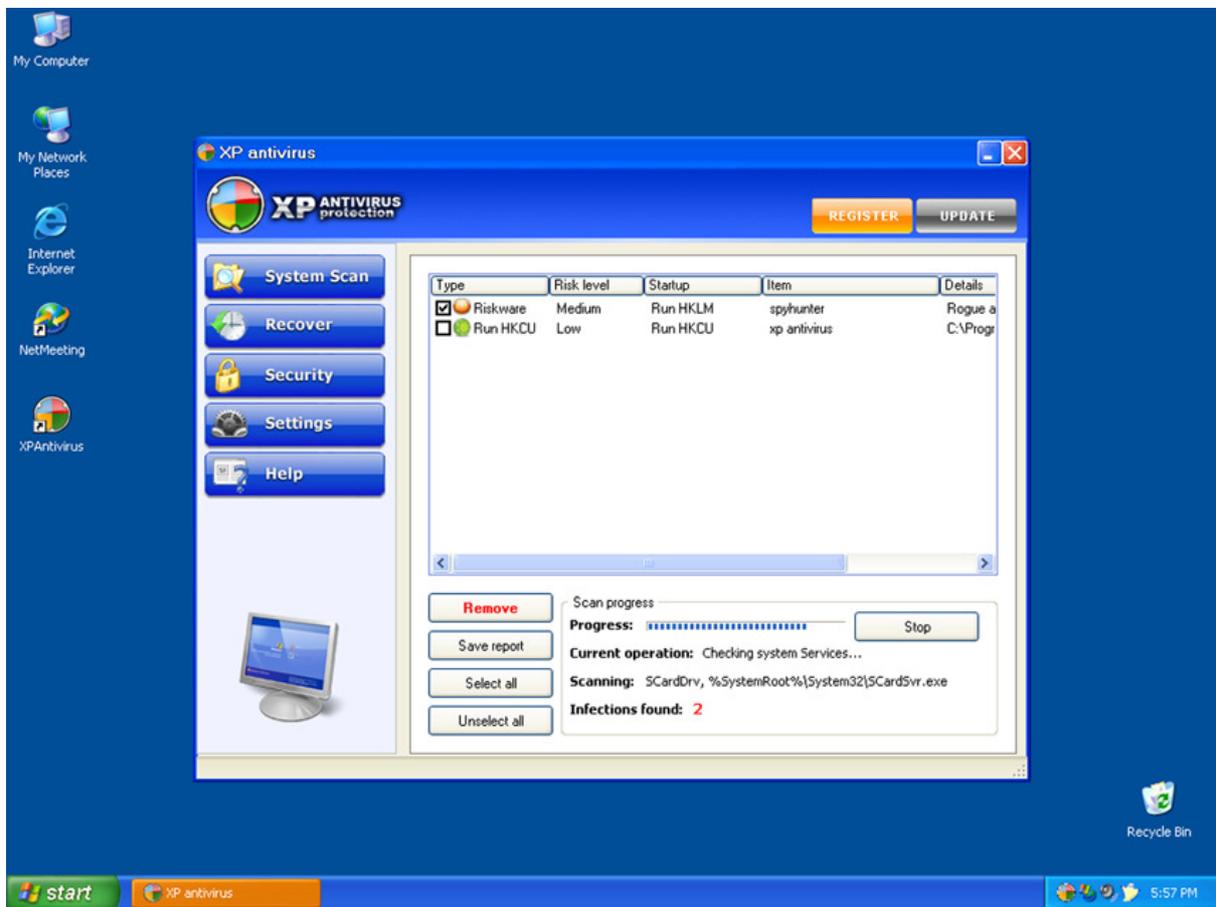
Above is a screenshot of the Rogue Software XP Antivirus