

Comodo Continues To Demonstrate Its Commitment To Secure All PCs With A New Suite of Testing Tools

Date: 04-21-2008 10:12 AM CET

Category: [IT, New Media & Software](#)

Press release from: [COMODO](#)

Agency: **COMODO**

New application can help technical community expose virus threats such as rootkit installations, commonly overlooked by many other testing tools

Jersey City, NJ (April 18, 2008) - Comodo, a leading security company, announced today the release of a new application which incorporates five new security and HIPS functionality tests. These tests, especially those that detect rootkit installations, incorporate techniques commonly used by virus authors and provide a very good indication of a security product's ability to block real-world threats. Comodo developed these tests largely so that it can deliver new preventative intelligence to end users on the performance of their PC security solutions before damage is done.

Comodo Malware Labs is constantly identifying techniques that malware authors use to bypass PC security solutions. One particularly damaging threat identified by Comodo engineers occurs when a rootkit is installed, without permission, on a user's system. Rootkits are the "ultimate backdoor" giving hackers ongoing and virtually undetectable access to the systems they exploit. Rootkits are so damaging because they compromise computer systems by subverting the Windows Kernel, the central component of most computer operating systems (OSs) which manages the system's resources and the communication between hardware and software components. In worse case situations, a PC can be rendered useless once it has been infected with a rootkit, as often this type of virus cannot easily be removed or quarantined. Therefore, it is critical that users have an easy means to test for this type of vulnerability before damage is done. It is Comodo's hope that end users who discover they are vulnerable to rootkit installations after running these new tests will take measures to upgrade or replace their security software.

This set of testing tools was designed to emulate different types of attacks and include the following tests:

- * Rootkit Installation 1 - Loads a driver in via ZwSetSystemInformation API. A very old, known and effective way to install a rootkit.
- * Rootkit Installation 2 - Loads driver by overwriting a standard driver (beep.sys) and starting it with service control manager (e.g. Trojan.Virantix.B).
- * DLL Injection 1 - Injects DLL into trusted process (svchost.exe) by injecting APC on LoadLibraryExA with "dll.dll" as a param. The string "dll.dll" is not written into process memory, it's from the ntdll.dll export table which has the same address in all processes. The APC is injected into second thread of the svchost.exe which is always in alertable state.
- * DLL Injection 2 - An old technique but very widespread technique. A DLL is injected via remote thread creation in the trusted process, without using WriteProcessMemory.
- * BITS Hijack - Downloads a file from the internet using "Background Intelligent Transfer Service" which acts from the trusted process (svchost.exe)

"Comodo's Labs identify many different techniques used by malware authors around the globe." said Melih Abdulhayoglu, CEO and Chief Security Architect of Comodo. "It is our hope that with these set of tests, users can be better informed about the state of their PC security and deliver this vital feedback back to their security providers. This is how we hope these tests will help drive better security solutions - industry wide."

The new Comodo HIPS and Firewall Leak Test Suite can be downloaded from the Comodo website at: personalfirewall.comodo.com/cltinfo.html

About Comodo

The Comodo companies provide the infrastructure that is essential in enabling e-merchants, other Internet-connected

companies, software companies, and individual consumers to interact and conduct business via the Internet safely and securely. The Comodo companies offer PKI SSL, Code Signing, Content Verification and E-Mail Certificates; award winning PC security software; vulnerability scanning services for PCI Compliance; secure e-mail and fax services.

Continual innovation, a core competence in PKI, and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo secures and authenticates online transactions and communications for over 200,000 business customers and 3,000,000 users of our desktop security products.

For additional information on Comodo - Creating Trust Online™ visit www.comodo.com

For more information, reporters and analysts may contact:

Judy Shapiro

Comodo

+1 (201) 963-9471

Email: judy.shapiro@comodo.com

COMODO Solutions

525 Washington Blvd

Jersey City, 07310

USA

The Comodo companies provide the infrastructure that is essential in enabling e-merchants, other Internet-connected companies, software companies, and individual consumers to interact and conduct business via the Internet safely and securely. The Comodo companies offer PKI SSL, Code Signing, Content Verification and E-Mail Certificates; award winning PC security software; vulnerability scanning services for PCI Compliance; secure e-mail and fax services.

[You can find this press release here](#)