Veracode Expands Leadership in Backdoors and Malicious Code Detection

Submitted by: Jane Folwell
Thursday, 5 March 2009

Industry’s Most Comprehensive Backdoor Coverage Protects Enterprises from New Threats

Burlington, Mass. – 5 March, 2009 – Veracode, the leading provider of on-demand application security testing solutions, today announced that it has expanded its coverage for detecting backdoors and malicious code embedded in legitimate software as part of Veracode’s SecurityReview® solution for developers and purchasers of software. This announcement builds upon Veracode’s industry-leading technology and research which introduced the industry’s first comprehensive taxonomy of backdoors in 2007.

Veracode has added the ability to detect growing threats commonly known as Time Bombs, Hardcoded Cryptographic Constants and Credentials, Deliberate Information and Data Leakage, Rootkits and Anti-Debugging techniques in applications. These targeted threats are hidden in software and mask their presence to evade detection by traditional security technologies. Coupled with Veracode’s existing detection capabilities, this forms the most complete support of backdoor and malicious code available in the market.

“Application backdoors and malicious code are risks for any large enterprise,” said Mark McGovern, at In-Q-Tel, the independent strategic investment firm that identifies innovative technology solutions to support the mission of the broader U.S. Intelligence Community and an investor in Veracode. “Automated tools that can look deeply into complex systems and assist managers in understanding hidden vulnerabilities such as backdoors are of significant interest. Manual processes don’t scale to meet industry needs. ”

The Defense Science Board Task Force has warned of this significant threat in its report “Mission Impact of Foreign Influence on DoD Software.” The report states that “High-end attackers will not be content to exploit opportunistic vulnerabilities, which might be fixed and therefore unavailable at a critical juncture. They may seek to implant a vulnerability for later exploitation.” Additionally, the SANS Institute recently issued “Application Security Procurement Language” which requires organizations to certify that their software does not contain malicious code, backdoors and time bombs. The State of New York and the Depository Trust and Clearing Corporation (DTCC) have adopted this language as a pre-requisite for vendors to do business with them.

“As organizations increasingly use third party service providers to design, build and manage their software applications, application security becomes ever more critical,” said Stan Lepeak, Managing Director of Global Research for EquaTerra. “Veracode’s application security testing services can help fill a hole that exists in too many enterprises’ testing and acceptance programs for third party developed code.”

“Modern software development is complex and comprised of outsourced code, open source and third party libraries, which makes the insertion of backdoors and malicious code difficult to detect by traditional source code analysis and thus, an attractive attack vector,” said Matt Moynahan, CEO of Veracode. “Unfortunately due to economic conditions and corporate downsizing, backdoors are becoming an increasing threat not only from external attackers, but from privileged insiders. Veracode inspects the application binary, which is the only way to cover 100% of the application code. Verifying the binaries as part of the SDLC or purchase process is the easiest and most effective way to manage risk from backdoor and malicious code vulnerabilities.

Availability

The new scanning technology to identify additional backdoors and malicious code will be available in Q2 2009. Veracode's SecurityReview is provided as an on-demand Software-as-a-Service (SaaS) solution, which means there is no on-premises hardware or software to upgrade or additional maintenance fees required for customers to take advantage of this enhanced functionality.

Multimedia

Download the podcast to hear more from Veracode on backdoors
Watch the Veracode Application Backdoor Webinar
Download a technical white paper to read about the taxonomy of backdoors
Download a white paper that examines the business risks associated with backdoors

About Veracode

Veracode is the world's leader for on-demand application security testing solutions. Veracode SecurityReview is the industry's first solution to use patented binary code analysis and dynamic web analysis to uniquely assess any application security threats, including vulnerabilities such as cross-site scripting (XSS), SQL injection, buffer overflows and malicious code. SecurityReview performs the only complete and independent security audit across any internally developed applications, third-party commercial off-the-shelf software and offshore code without exposing a company's source code. Delivered as an on-demand service, Veracode delivers the simplest and most-cost effective way to implement security best practices, reduce operational cost and achieve regulatory requirements such as PCI compliance without requiring any hardware, software or training.

Veracode has established a position as the market visionary and leader with awards that include recognition as a Gartner "Cool Vendor" 2008, The Banker Technology award for Information Security Project of the Year 2008, SC Magazine Europe awards 2008 for Innovation and also for Best Vulnerability Assessment, Wall Street Journal's Technology Innovation Award, Info Security Product Guide's "Tomorrow's Technology Today Award 2008," Information Security "Readers' Choice Award 2008," AlwaysOn Northeast's "Top 100 Private Company 2008", NetworkWorld "Top 10 Security Company to Watch 2007," and Dark Reading's "Top 10 Hot Security Startups 2007."

Based in Burlington, Mass., Veracode is backed by In-Q-Tel, .406 Ventures, Atlas Venture and Polaris Venture Partners. For more information, visit www.veracode.com.

###

Contact:

Jane Folwell, Folwell PR
Tel: 01344 845132
Mob tel: 07950 033370
Email: jane@folwellpr.co.uk

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of Jane Folwell