VERACODE SHINES SPOTLIGHT ON SOFTWARE BACKDOORS AS EMERGING THREAT

Submitted by: Jane Folwell

Tuesday, 5 February 2008

Exciting innovator in application security testing heals pain points with first online based subscription service for testing software code

Burlington, Mass., 5 February 2008 – Veracode, the first provider of on-demand application security testing solutions, today announced a further innovation – comprehensive detection of backdoors and malicious code. Veracode is the only company to offer application code reviews on a software-as-a-service subscription basis. Veracode's SecurityReview® is the first solution to enable organisations to discover security flaws in software automatically, without releasing their valuable source code. Whether a company is buying or building software Veracode helps improve the security quality of applications without the need to hand over precious intellectual property by providing comprehensive identification and remediation of the security flaws contained in binary code, the very foundation of today's software applications.

The addition of the new backdoor detection capability further strengthens Veracode's position as a true trailblazer in the application security arena. Backdoors are often included in programmes by developers for seemingly legitimate purposes but are increasingly being exploited by hackers to compromise applications. Research from the US Department of Homeland Security points to a significant risk from backdoors and 23% of software packages used by US government employees have backdoors built into them.

"Backdoors and malicious code pose significant operational risk to enterprises and software that are just too significant to ignore," said Matt Moynahan, chief executive officer of Veracode. "Given the complexity of modern application development, the common practice of outsourcing and increasing use of third party libraries, it is nearly impossible for an enterprise to identify the pedigree and security level of the software running their business-critical applications and handling their customer's personally identifiable information. As a result, we expect backdoors and malicious code insertion to become an increasingly prevalent attack vector against the enterprise. Because the binary (compiled code) represents the actual attack surface for the hacker, testing the application binaries is the most accurate and complete way to conduct final, independent security validation and verification."

As the complexity of modern software applications increases, with components assembled from reusable binary components, backdoors can easily circumvent even the best of QA cycles, resulting in the need for a more complete and accurate approach to software security testing. Veracode's binary software testing, which provides 100% coverage as opposed to the partial coverage of today's source code-only analysis solutions, is uniquely positioned to tackle the backdoors and malicious code challenge by offering a complete, independent security verification of an entire software application.

On the back of extensive research, Veracode has developed the first comprehensive taxonomy of backdoors so that organisations and application developers can better understand how to detect these hidden threats. Veracode has found that the average time to discovery of a backdoor inserted in open source software was measured in weeks. Backdoors in commercial "closed source" applications went undetected for years, putting company and individuals' personal data at risk.

SecurityReview is now fully available in Europe.

For more information on Veracode's software backdoor capabilities, please visit us at http://www.veracode.com/. .

Multimedia

Download - the podcast or visit the blog to hear more from Veracode on backdoors
Download - technical white paper to read about the taxonomy of backdoors
Download - white paper that examines the risks associated with backdoors

Definitions

• Special Credential Backdoors – These occur when an attacker inserts logic and special credentials into the program code. The special credentials are in the form of a username, password, password hash, or key which is usually hardcoded. Special credentials are also inserted by developers for the purpose of customer support or for debugging. These pose a similar risk since once they are discovered attackers can use them as a backdoor.

• Hidden Functionality Backdoors – These allow the attacker to issue commands or authenticate without performing the designed authentication procedure. Hidden functionality backdoors often use special parameters to trigger logic within the program that is not intended. In web applications these are often invisible parameters for web requests (not to be confused with hidden fields). Other hidden functionality includes undocumented commands, hardcoded IP addresses and/or leftover debug code.

• Rootkits – Rootkit behavior in an application can be a warning that a backdoor or other malicious code may be present. Typically rootkits subvert functions of the operating system and are used to hide the backdoor. This helps attackers subsequently access the system and avoid detection.

• Unintended Network Activity – Unintended network activity is a common characteristic of backdoors. This may involve a number of techniques, including listening on undocumented ports, making outbound connections to establish a command and control channel, or leaking sensitive information over the network via SMTP, HTTP, UDP, ICMP, or other protocols. Occasionally this will be an intended feature of the software for use as a support mechanism but it can carry security and privacy risks and should be detected.

About Veracode

Veracode is the leading US provider of on-demand application security testing solutions. Created by a world-class team of application security experts, the company was launched in the US last year to deliver services to identify software flaws introduced through coding errors or malicious intent. Veracode's core service, SecurityReview uses patented binary code analysis and dynamic web analysis that is uniquely able to inspect entire application inventories, including components, and does not require companies to expose their valuable source code. Enterprises can now protect their intellectual property while preventing attacks allowed by vulnerabilities in applications. SecurityReview is already gaining strong traction in

the North American market (customers include two billion dollar Canadian telecoms company, TELUS) and is currently being taken by a leading financial organisations in the UK.

As the most accurate and comprehensive solution, Veracode makes it simple and cost-effective to implement application security best practices and reduce operational costs related to manual reviews. Whether a company is developing applications internally, purchasing software or integrating code from partners, Veracode's SecurityReview provides insight to the security level of your applications. Outsourcing code analysis to Veracode is the easiest way to secure your software. With a pragmatic approach to application security, Veracode helps you fix what matters most to your business.

Based in Burlington, Mass., Veracode is backed by .406 Ventures, Atlas Venture and Polaris Venture Partners. http://www.veracode.com/

Media Contacts:

Jane Folwell
Folwell PR
Tel: (44) (0)1344 845132
Mob tel: (44) (0)7950 033370
Email: jane@folwellpr.co.uk