

VERACODE
VERACODE
VERACODE

Joe Brady
Senior Solutions Architect

jbrady@veracode.com



VERACODE
VERACODE
VERACODE

Detecting Software Backdoors

Austin OWASP
August 30, 2011

VERACODE
Software Security Simplified

Joe Brady
Senior Solutions Architect
jbrady@veracode.com

- **Veracode** provides automated, SaaS-based, application security assessment and remediation capabilities for **Internal, external** and **3rd party Applications**.
- Automated techniques include **static binary analysis** and **dynamic analysis**.
- Founded in 2006, includes application security experts from L0pht, @stake, Guardent, Symantec, VeriSign and SPI Dynamics/Hewlett Packard



Now is a good time to think about software backdoors



- Unverified and untested software is everywhere
- It's in your computer, house, car, phone, TV, printer and even refrigerator
- Most of that software was developed by people you don't trust or don't know very well
- You clicked on that link someone sent you didn't you?

What we will cover today (three things to ~~worry~~ think about)



- Application Backdoors
 - Backdoors in the applications you own, are buying or have built
 - Do you know where your source code was last night?
- System Backdoors
 - Vulnerabilities in the software you use everyday that can be used to implant a system backdoor
 - E.g. Aurora (CVE-2010-0249)
- Mobile Backdoors
 - Your phone just might be spying on you



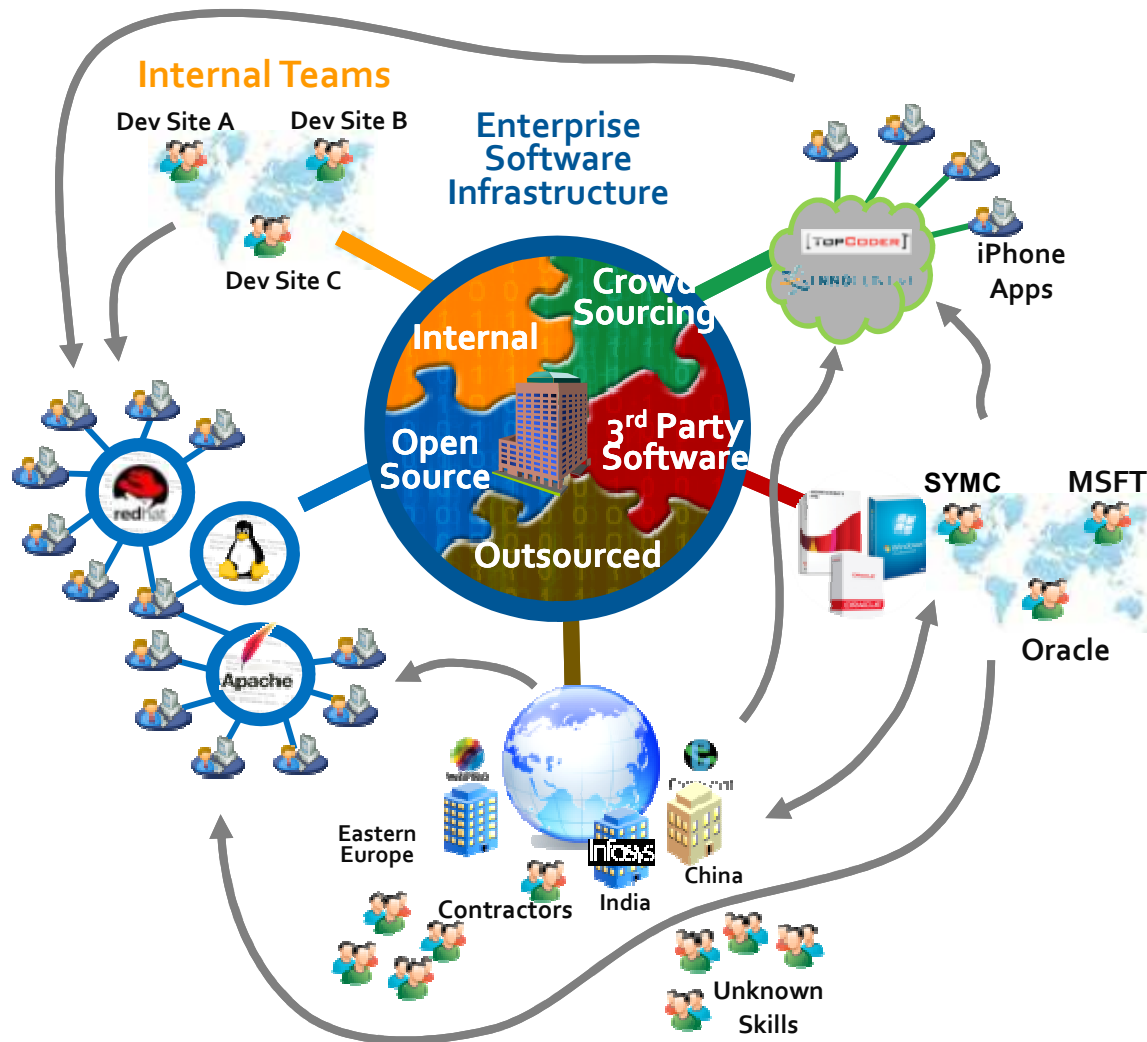
Attacker Motivation

- Most practical method of compromise for many systems
 - Let the users install your backdoor on systems you have no access to
 - Looks like legitimate software so may bypass AV
- Retrieve and manipulate valuable private data
 - Looks like legitimate application traffic so little risk of detection by IDS and DLP
- For high value targets it becomes cost effective and more reliable.
 - *“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 vulnerability for later exploitation.”*

from report of the Defense Science Board Task Force, “Mission Impact of Foreign Influence on DoD Software”

How?

Complex Software Ecosystem creates lots of Opportunities



Apps are:

- Targets by Design

- Re-usable by Design

- 3rd-party by Design



Application Backdoors

A Few Examples

Maybe I Needing Later?



```
// maybe I needing later
if ($_GET['page'] ==
delete_all_files") {
    echo "del";
    mysql_query("DROP TABLE *");
    unlink("index.php");
    unlink("apps.php");
    unlink("resources");
    ... snip all files ...
}
```

Code from: <http://thedailywtf.com/Articles/Maybe-I-Needing-Later.aspx>

Maybe your Applications are Certified “Pre-Øwned?”



- Software or hardware that comes with malicious behavior right out of the box.
- Historical listing Available
 - <http://attrition.org/errata/cpo/>
- Energizer DUO USB Battery Charger software
 - **March 5, 2010**
 - Installs backdoor that allows remote user complete control of system
 - Direct from the manufacturer!

Backdoor in Commercial Software == Data of 35M Users Stolen

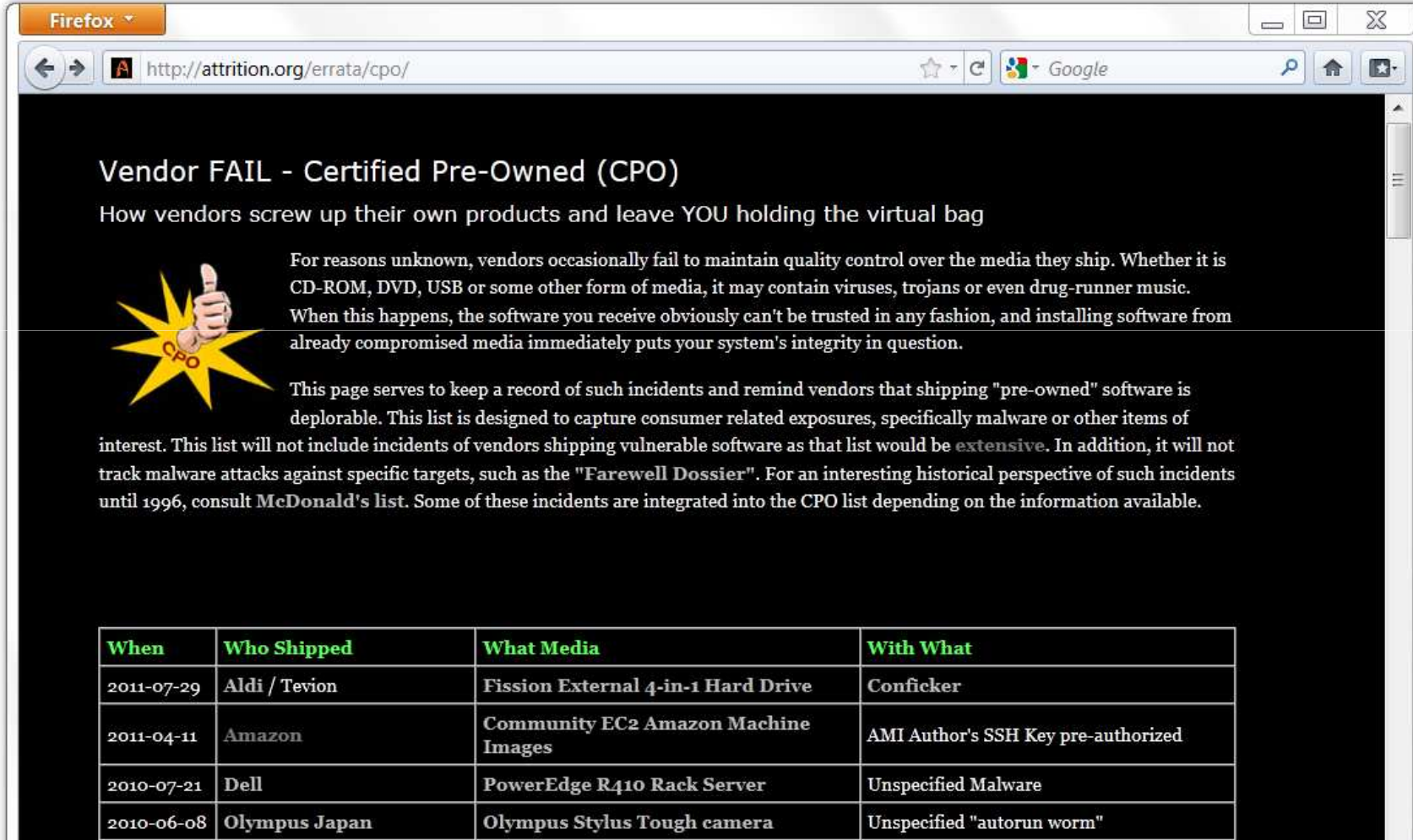


- Account names, passwords, email address, and other info stolen from 35M users at Korean social networking site owned by SK Communications (July 28, 2011).



- ESTsoft Alzip distribution site compromised and backdoor installed. ESTsoft is also antivirus vendor.
- Backdoor contacts C&C server, accesses database, and exfiltrates data.

List of Certified Pre-Owned (CPO) on attrition.org



Vendor FAIL - Certified Pre-Owned (CPO)
How vendors screw up their own products and leave YOU holding the virtual bag

For reasons unknown, vendors occasionally fail to maintain quality control over the media they ship. Whether it is CD-ROM, DVD, USB or some other form of media, it may contain viruses, trojans or even drug-runner music. When this happens, the software you receive obviously can't be trusted in any fashion, and installing software from already compromised media immediately puts your system's integrity in question.

This page serves to keep a record of such incidents and remind vendors that shipping "pre-owned" software is deplorable. This list is designed to capture consumer related exposures, specifically malware or other items of interest. This list will not include incidents of vendors shipping vulnerable software as that list would be *extensive*. In addition, it will not track malware attacks against specific targets, such as the "Farewell Dossier". For an interesting historical perspective of such incidents until 1996, consult McDonald's list. Some of these incidents are integrated into the CPO list depending on the information available.

When	Who Shipped	What Media	With What
2011-07-29	Aldi / Tevion	Fission External 4-in-1 Hard Drive	Conficker
2011-04-11	Amazon	Community EC2 Amazon Machine Images	AMI Author's SSH Key pre-authorized
2010-07-21	Dell	PowerEdge R410 Rack Server	Unspecified Malware
2010-06-08	Olympus Japan	Olympus Stylus Tough camera	Unspecified "autorun worm"

Don't forget Application Plugins/Add-ons/Links



- Application Plugins
- Browser plugins
- Video codecs
- Even “bookmarklets”
 - <http://ha.ckers.org/blog/20100126/quicky-firefox-bookmarklet-backdoor/>

Example: Master Filer Firefox Add-On



- Once computer infected, locates a running web browser to inject code into it
- Communicates with Outlaw server
- The backdoor to execute a number of actions such as copying, deleting, renaming, finding and executing files; download and upload files; modify the Windows Registry; and create screenshots of a desktop.
- On download site for 5 months



System Backdoors

Our Old Favorite

System Backdoors



```
<script>
var c = document
var b = "60 105 [...encrypted bytes removed...] 62 14 10 "
var ss=b.split(" ");
var a ="a a a [...removed bytes...]| } ~ "
var s=a.split(" ");
s[32]=" "
cc = ""
for(i=0;i<ss.length-1;i++) cc += s[ss[i].valueOf()-i%2];
var d = c.write
d(cc);
</script>
```

Aurora code sample

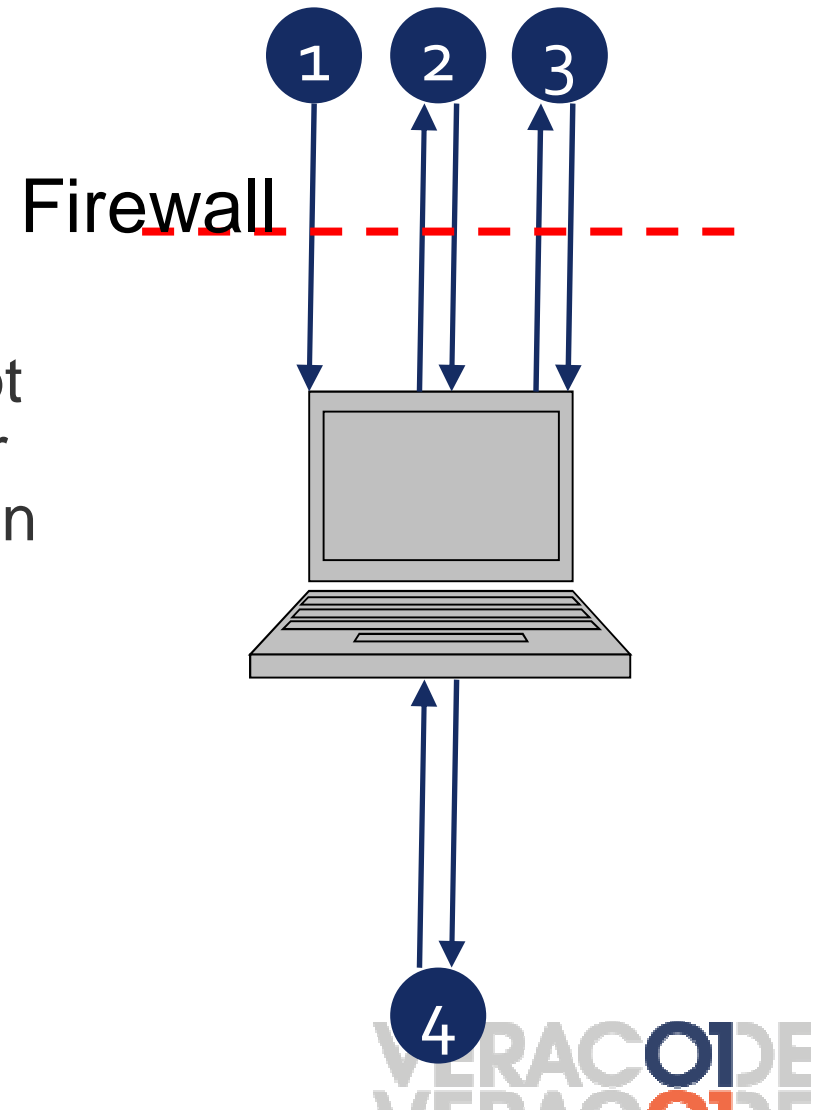
Weapon of Choice : Operation Aurora

- Google perimeter is breached via a vulnerability in Microsoft IE6 (installed as part of the OS)
- Attack is named “Aurora” after the remote access malware installed
- Microsoft describes vulnerability:

“A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution.”
- At least 34 companies known to be affected
- Attackers targeted source code

Aurora Attack Vector Illustrated

1. URL sent to victim via email, social networking, or through a web application vulnerability such as XSS
2. Victim views malicious web page, which contains Javascript code that exploits the Use After Free bug in IE and installs trojan backdoor on victim's machine
3. Compromised machine communicates out to C&C server
4. Attackers access internal network





Mobile Backdoors
There's an App for that!

An Emerging Threat

Mobile Spyware

- Often includes modifications to legitimate programs designed to compromise the device or device data
- Often inserted by those who have legitimate access to source code or distribution binaries
- Not specific to any particular mobile Operating System



Data Leakage: Mobile App Specific

Sensitive Data

Monitor connected / disconnected calls
Monitor PIM added / removed / updated
Monitor inbound and outbound SMS
Real Time track GPS coordinates
Dump all contacts
Dump current location
Dump phone logs
Dump email
Dump microphone
Dump current camera

Communications Channel

SMS (No CMDA)
SMS Datagrams (Supports CDMA)
Email
HTTP GET
HTTP POST
TCP Socket
UDP Socket

Veracode TXSBBspy

- Proof of concept mobile backdoor/spyware
- Video demo and source code available on <http://www.veracode.com/blog/>
- No attempt to hide itself. C&C over SMS text
- Uses only legitimate RIM APIs
- Tracks your location, bugs your room, reads all your email

Mobile Backdoor Example: Storm8 Phone Number Farming

- iMobsters and Vampires Live (and others)
 - “Storm8 has written the software for all its games in such a way that it automatically accesses, collects, and transmits the wireless telephone number of each iPhone user who downloads any Storm8 game,” the suit alleges. “ ... Storm8, though, has no reason whatsoever to access the wireless phone numbers of the iPhones on which its games are installed.”
- “Storm8 says that this code was used in development tests, only inadvertently remained in production builds, and removed as soon as it was alerted to the issue.”
- These were available via the iTunes App Store!
 - <http://www.boingboing.net/2009/11/05/iphone-game-dev-accu.html>

Mobile Backdoor Example: 09Droid – Banking Applications Attack



- ▶ Droid app that masquerades as any number of different target banking applications
- ▶ Target banks included
 - Royal Bank of Canada, Chase, BB&T, SunTrust, etc...
 - Over 50 total financial institutions were affected
- ▶ May steal and exfiltrate banking credentials
- ▶ Approved and downloaded from Google's Android Marketplace!
 - <http://www.theinquirer.net/inquirer/news/1585716/fraud-hits-android-apps-market>
 - <http://www.pcadvisor.co.uk/news/index.cfm?RSS&NewsID=3209953>
 - <http://www.f-secure.com/weblog/archives/00001852.html>



Backdoor Detection

Addressing the Problem

Special Credentials

- Special credentials, usually hard-coded, which circumvent security checks
 - Usernames
 - Passwords
 - Secret hash or key



The Keymaker from “The Matrix Reloaded”

He is able to make keys that get him into secret areas of the Matrix.

Hidden Functionality

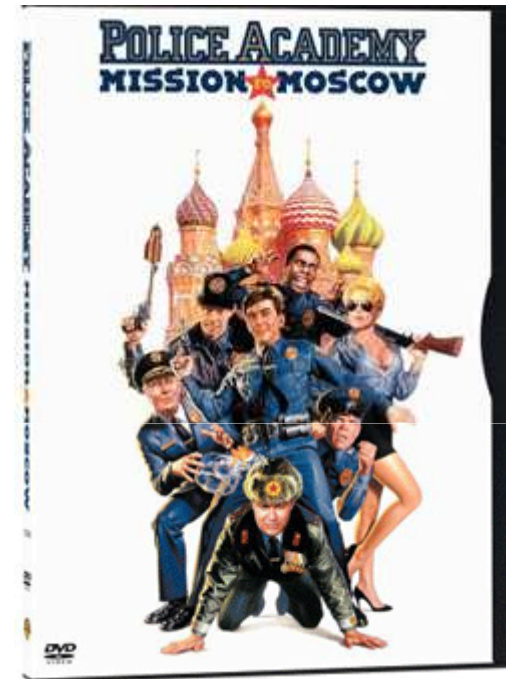
- Invisible parameters in web applications
 - not to be confused with hidden form fields
- Undocumented commands
- Leftover debug code
 - e.g. WIZ command in early sendmail
- May be combined with “special” IP addresses



Number Six, a Cylon Agent, from Battlestar Galactica
In exchange for access to government mainframes she helps design the navigation program subsequently used by Colonial warships, covertly creating backdoors in the program.

Unintended Network Activity

- Listens on an undocumented port
- Makes outbound connections
- Leaks information over the network
 - Reads from registry, files, or other local resources
 - Sends data out via SMTP, HTTP, UDP, ICMP, or other protocols
- Potentially combined with rootkit behavior to hide the network activity from host-based IDS



In the movie, Konstantin Konali markets a computer game that everyone in the world is playing. With a sequel to the game he wants to put backdoors in all computer systems on which it gets installed, thus providing access to the police and other government systems.

Look for indicators of malicious code

- Indicators are not malicious by themselves but they often coincide with malicious code.
- They obfuscate behavior from dynamic or static analysis.
- Categories
 - Rootkit behavior
 - Anti-debugging
 - Time bombs
 - Code or data anomalies

Current State of Detection

- Almost all backdoor detection done today is through manual code review
 - This doesn't scale, is difficult and expensive
- Application backdoors or data leakage best detected by inspecting the source or binary code of the program
 - Dynamic web application scanners are almost 100% ineffective yet this is what the majority of companies use for application testing
- Most security reviews focus on finding vulnerabilities with little emphasis on backdoors and data leakage
- Mobile application static analysis is available but no app stores have incorporated this into their approval process...yet.
 - You have to trust the app store!

Automating the Backdoor Detection Process is Key

- Without automation, the task of analyzing all applications for backdoors is likely impossible
 - Only recently has the technology become available to address this challenge
- Static Analysis solutions can be equipped to look for backdoors and automate the process
 - Binary Analysis solutions can process hundreds of applications per month regardless of size without requiring source code and with greater accuracy
- For high risk applications automation should be followed up with manual inspection

When To Scan For Backdoors?

- **Before you buy the software**
 - Require your vendors have their applications scanned with every major release
- **During Development**
 - Incorporate detection and security testing into your software development lifecycle
- **Security Acceptance testing of outsourced applications**
 - Require a security and backdoor acceptance test before you take ownership or purchase
- **Don't trust Developers to test their own code, require a 3rd party**
 - Ken Thompson's paper, "Reflections on Trusting Trust"
<http://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf> /
 - Thompson not only backdoored the compiler so it created backdoors, he backdoored the disassembler so it couldn't be used to detect his backdoors!

Conclusion

- Backdoors are prevalent and increasing in frequency and complexity
- We are currently trusting the vendor application store provider for the majority of our mobile device security
- A number of automated means to verify application behavior and detect backdoors exist
- You should Incorporate security testing including backdoor detection into your SDLC and software acquisition process

Thank You



www.veracode.com



jbrady@veracode.com

VERACODE
Software Security Simplified

Report Available at
Veracode.com

