Protecting the Enterprise: Software Backdoors

VERACODE
•*Software Security Simplified*

Clint Pollock
Senior Solutions Architect
cpollock@veracode.com

Now is a good time to think about 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?**

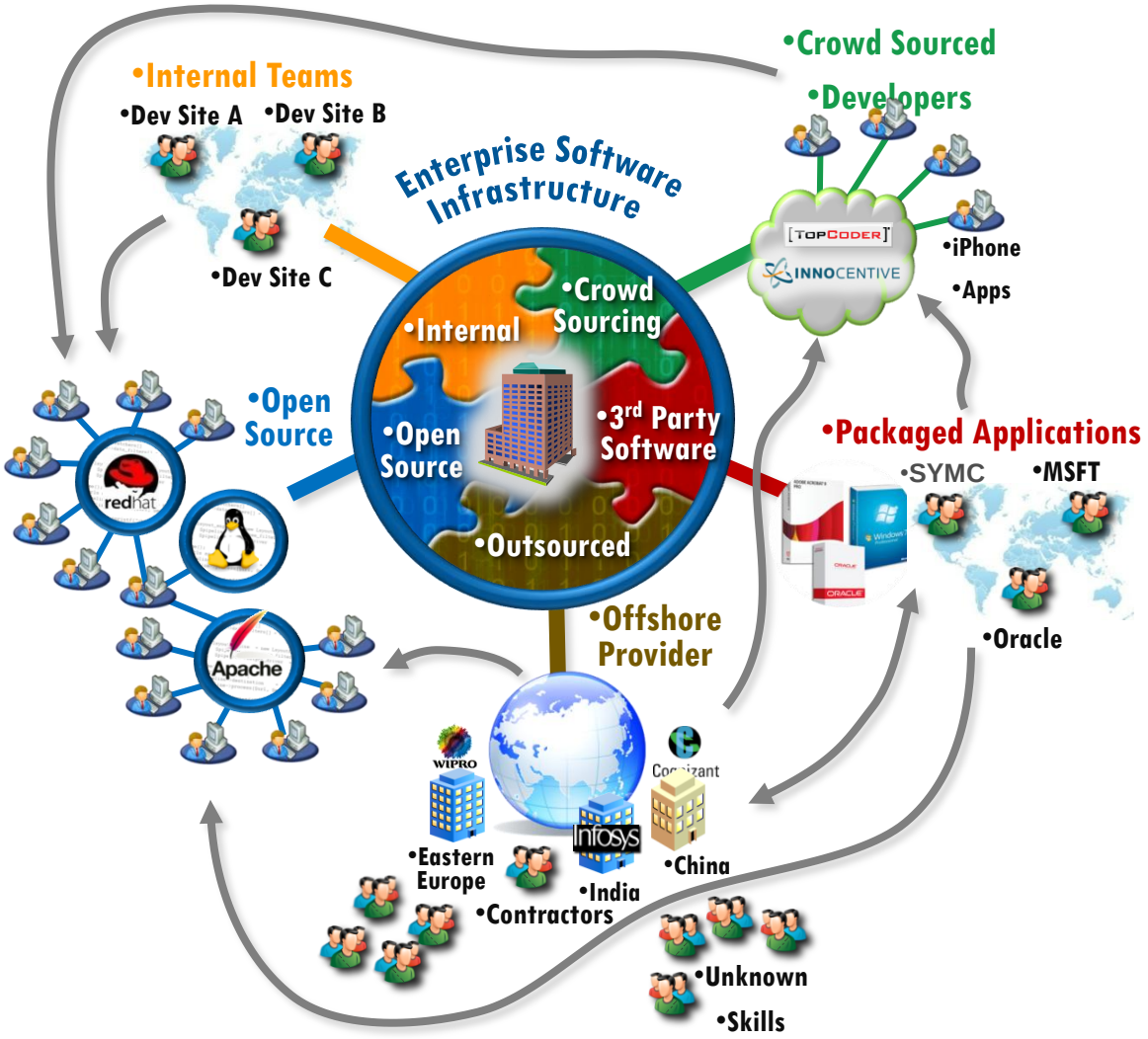
Three Things to ~~Worry~~ Think About

- 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

Why

- 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
- For high value targets such as financial services and government 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
  - It's not about getting root, it's about owning the system for life

The Picture As We See It



- •Apps are:
  - • Targets by Design
  - • Re-usable by Design
  - • 3rd-party by Design
- •VULNERABLE BY DESIGN!

Typical Backdoor functions

- Sending/ receiving files
- Launching/ deleting files
- Executing files
- Displaying notification
- Deleting data
- Rebooting the machine
- Keystrokes
- Screenshots

- More common in COTS and Internally developed Applications
- Open source applications are relatively free of backdoors

Application Backdoors

VERACODE

```
// 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

Are your Applications Certified "Pre-Øwned?"

- Energizer DUO USB Battery Charger software
  - **March 5, 2010**
  - Installs backdoor that allows remote user complete control of system
  - Download and execute files, directory listings, and send files
  - Direct from the manufacturer!
  - Existed since May 2007

Certified “Pre-Øwned”

- Software or hardware that comes with malicious behavior right out of the box.
- Historical listing http://attrition.org/errata/cpo/
- Some examples:
  - Samsung digital photo frame infected with Sality Worm
  - Walmart Promo CD included custom spyware
  - Sony BMG CDs included XCP rootkit
  - Borland Interbase backdoor password
  - Android “First Tech Credit Union” banking app

Don’t forget Application Plugins/Add-ons

- Remember that plugins and codecs are code too
- Example: Master Filer add-on for Firefox
  - Discovered to have trojan embedded on Jan 25, 2010. Add-on removed from distribution site.
  - Win32.Bifrose.32.Bifrose Trojan executes on first add-on startup.
  - Firefox scans add-ons when submitted but missed this one.

Master Filer Add-On

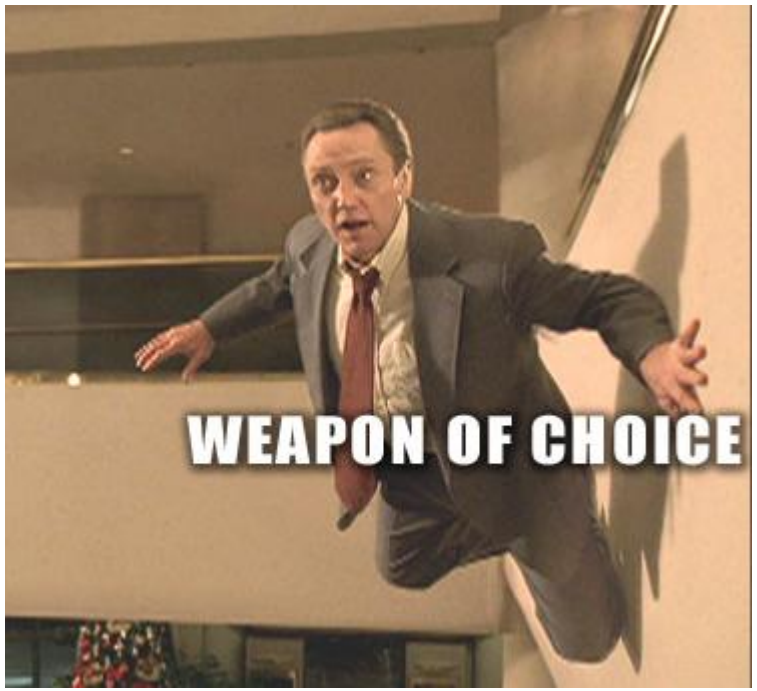
- Once computer infected, locates a running web browser to inject code into it
- Communicates with Outlaw server
- The backdoor to execute a number of actions such as copying, deleting, renaming, finding and executing files; download and upload files; modify the Windows Registry; and create screenshots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

What About Your Own Source Code?

- 3rd party code? External contractors or disgruntled employees? Cylon Agents?
- If a backdoor was added would you be able to find it?
  - Borland Interbase backdoor went undiscovered for 7 years
  - Searching for backdoors might be the only way to know you have been hacked
  - Unfortunately most code reviews do not look for backdoors

Cylon Agent Number Six from Battlestar Galactica designed the navigation program used by Colonial warships, covertly creating backdoors in the program.

Software Vulnerabilities + Backdoor = Weapon of Choice



- It's not about getting root on systems anymore
  - It's about taking control of your users machines and getting to their data
- *"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."*

  - Report of the Defense Science Board Task Force, "Mission Impact of Foreign Influence on DoD Software":

System Backdoors

VERACODE

```
<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

Operation “Aurora”

- Began in December 09 through February 2010
- Exploits a zero-day flaw in Internet Explorer to load the backdoor “Trojan.Hydraq” and take control of a users computer to steal intellectual property. (CVE-2010-0249/MS10-002)
- Used by China-based attackers to compromise systems at Google and up to 33 other companies
- Source code repositories were one of several targets of the attackers
- Microsoft knew about issue since September.
- Leveraged encryption to hide itself
- Outbound connection looks like standard SSL

Mobile Devices

VERACODE

Want to get hacked?

There's an app for that!

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 at http://www.veracode.com/blog/2010/02/is-your-blackberry-app-spying-on-you/
- No attempt to hide itself.
- 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
  - 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

VERACODE

Rootkit Behavior

VERACODE

- Modifies OS behavior
- Hides program behavior from system administration tools or other instrumentation

Anti-debugging

VERACODE

- Anti-debugging is the implementation of one or more techniques within computer code that hinders attempts at reverse engineering or debugging a target binary.
- Used by commercial executable protectors, packers, and malicious software, to prevent or slow-down the process of reverse-engineering.

Time Bombs

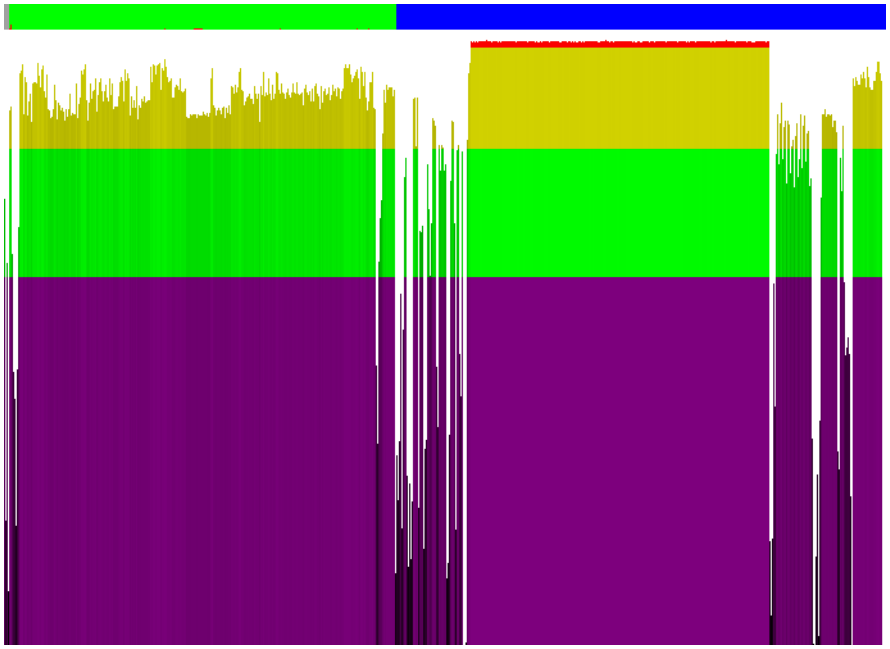
VERACODE

- A piece of code intentionally inserted into a software system that will set off a malicious function when specified time based conditions are met

- Program behavior to look for
  - Time comparison functions
  - Time retrieval functions

Code or Data Anomalies

VERACODE



•Entropy graph of executable

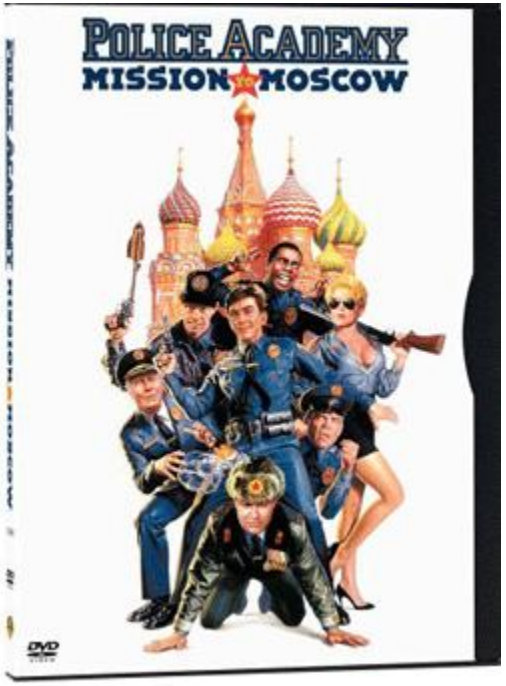
- Self-modifying code
  - Calling eval(obfuscated code) in scripting languages
  - Writing into code pages or jumping/calling into data pages
- Unreachable code
  - May be part of a two-stage backdoor insertion where code is added later that calls the unreachable code
- Encrypted blocks of data

Hidden Commands

- 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

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.

Current State of Detection

- Virus scanning for workstations
- SANS: Many more application backdoors than OS backdoors
- 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 Backdoor Detection

- Manual code review of all applications, while currently the best approach, is impossible
- Static **Binary** Analysis designed to look for backdoors can automate the process
  - Static Binary Analysis can process hundreds of applications per month.
  - Ensure you look at the entire application in its final form
  - Dynamic won't help.
- For high risk applications automation should be followed up with manual inspection

Static Binary Analysis

- Binary Modeling & Analysis
  - Provides accurate & comprehensive analysis because binary modeling renders a more accurate application data and control flow model
  - Includes analysis of libraries including inter-procedural flows
  - Both internal and external use cases (internal code; vendor code; mergers & acquisitions).
- Backdoors
  - Uniquely designed to detect backdoors that are only exposed in binaries of application
  - For example, hashed hard-coded passwords etc.
  - Detects backdoors inserted at compile time

When To Scan For Backdoors?

- Before you buy the software
  - Code delivered to you as .exe, .dll, .lib, .so
  - Require your vendors have their applications scanned with every major release
- During Development
  - Scan the code you are developing or maintaining at each milestone and before release
- Security Acceptance testing of outsourced development
  - Require a security and backdoor acceptance test before you take ownership
- Don't trust the 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

- Use automated testing methods to scale
- Static Binary Analysis is the most complete and accurate method you can use to detect backdoors across your final application.
- Analyze the application in its final form

Upcoming Webinars:

- May 6 - Application Security, reasons to worry
- May 20th – Training for secure code development
- June 3rd – Managing 3rd party application risk

Email cpollock@veracode.com

Thank You

VERACODE

Software Security Simplified