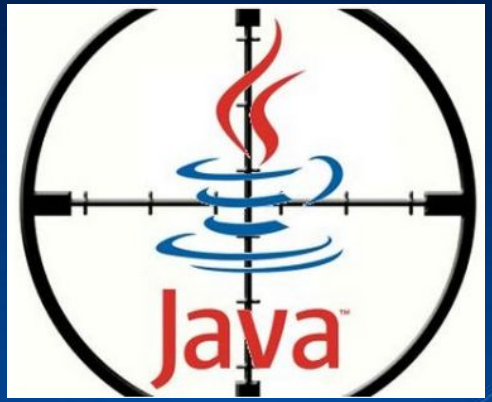


(IN)SECURITY OF JAVA

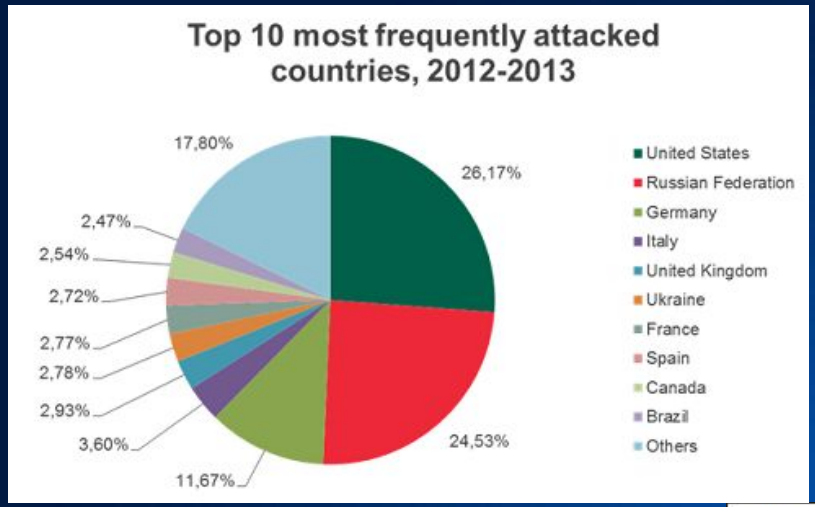
BY: Daniel Palombo, Raghad Khudher, Jamson Sor

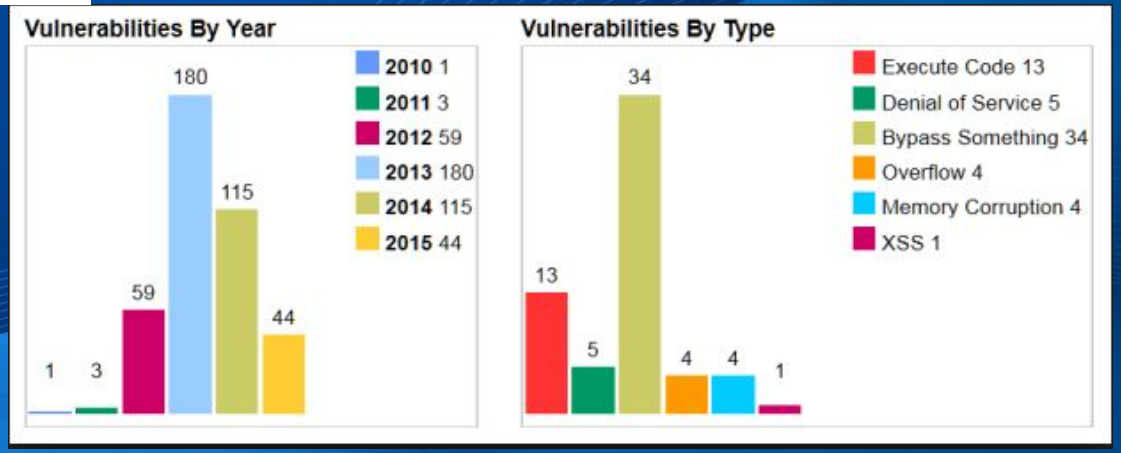
What is Java?

- Java is a programming language that developers use to create applications.
- Java was first publically released in 1995, it was revolutionary and ahead of its time!
- Java is not the same as JavaScript, there are many development languages out there
  including JavaScript, C, C++, Ruby, PHP, Scala, Python ...ect.
- Java has two ways of running applications. Directly on your computer or via the web browser.

What is the problem?

- When people talk about Java being insecure, they're talking about the browser plug-in. Java apps themselves are not inherently insecure!
- The java browser plug-in is a notoriously insecure piece of software. It has many vulnerabilities which haven't been fixed in the years to come.
- According to Kaspersky, it’s responsible for almost 50% of cyber attacks in 2012.


Top 10 most frequently attacked countries, 2012-2013
17,80%
26,17%
2,47%
2,54%
2,72%
2,77%
2,78%
2,93%
3,60%
24,53%
11,67%
United States
Russian Federation
Germany
Italy
United Kingdom
Ukraine
France
Spain
Canada
Brazil
Others


Vulnerabilities By Year
2010 1
2011 3
2012 59
2013 180
2014 115
2015 44
1
3
59
180
115
44
Vulnerabilities By Type
Execute Code 13
Denial of Service 5
Bypass Something 34
Overflow 4
Memory Corruption 4
XSS 1
13
5
34
4
4
1

Is Java less secure than the other development languages?

- The answer is a clear-cut 'NO!'. If the answer would have been yes, you'd probably want to throw away your DVD and Blue-Ray players, your refrigerators, phones,
  cars and many other devices that run Java.
- Security issues have long tantalized over 850 million users that have Oracle's Java software installed on their computers. The worst thing is that the software was not fully updated or secure for years, exposing millions of PCs to attack.

- Oracle is settling with the Federal Trade Commission (FTC) over charges that it "deceived" its customers by failing to warn them about the security upgrades.

After all, why would so many people choose to use software that has frequent security holes?

According to Oracle:

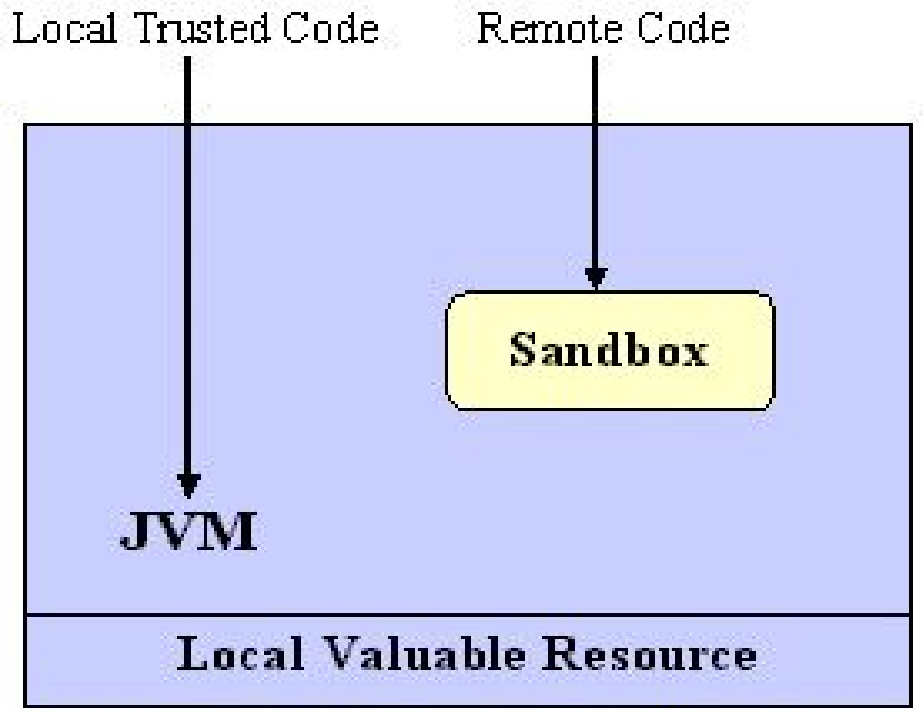
- 97% of Enterprise Desktops Run Java
- 89% of Desktops (or Computers) in the U.S. Run Java
- There are 9 Million Java Developers Worldwide
- Java is the #1 Choice for Developers
- Java is the #1 Development Platform
- 3 Billion Mobile Phones Run Java
- 100% of Blu-ray Disc Players Ship with Java
- There are 5 Billion Java Cards in Use
- 125 million TV devices run Java
- And 5 of the Top 5 Original Equipment Manufacturers Ship Java ME.

How is Java secure?

- Untrusted code from websites are run in a sandboxed environment.

- Only code that is run locally will have access to local resources

- An applet must have users approval In order to operate outside the sandbox



How is Java insecure?

1) Vulnerabilities / bugs allow code to run outside the sandbox.

2) Social Engineering can be used to make users give malicious applets higher privileges.

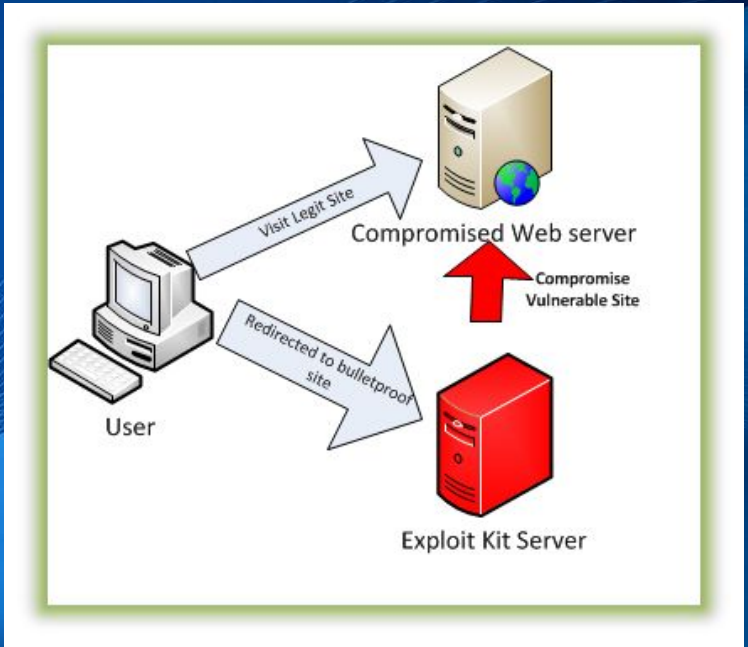
How are Java vulnerabilities exploited?

The process is automated using exploit kits

- When you visit a compromised website, your browser is redirected to a server that hosts an exploit kit.

- Javascript is used to determine the version of your Java plug-in

- The exploit kit attempts to exploit that versions known vulnerabilities



How are Java vulnerabilities exploited?

- A web browser with an outdated Java version is an easy target.

- The payload (Malware) is dropped into the system to perform malicious actions.

How social engineering is used

- User receives seemingly legitimate link to a malicious website through email.

- Java applet requests user permission to run.

- When user gives permission, the applet then has access to the system that would be otherwise protected by the sandbox.

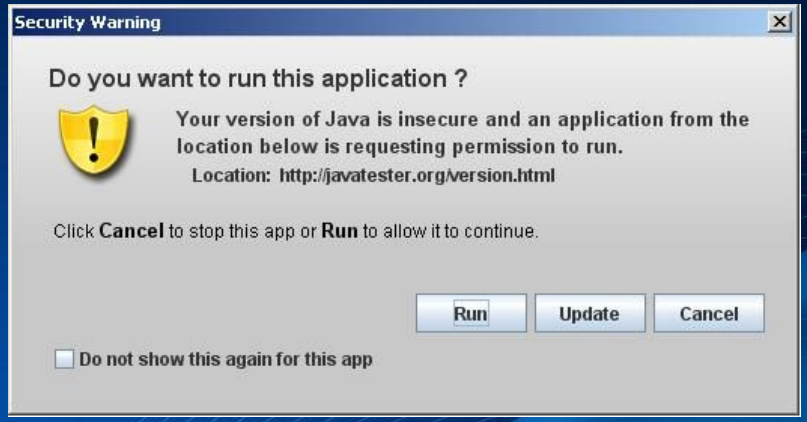
Exploiting vulnerabilities is most common

Exploiting vulnerabilities in Java is beneficial to the attacker since the victim doesn’t need to give authorization, which makes them more likely to be unaware of the attack.

Days since last known Java 0-day exploit

Previous high score: 723 (up from 87)

- Java SE updates did not remove earlier versions of itself, only the most recent version
- Exposed the system to vulnerabilities from the older versions still on the system

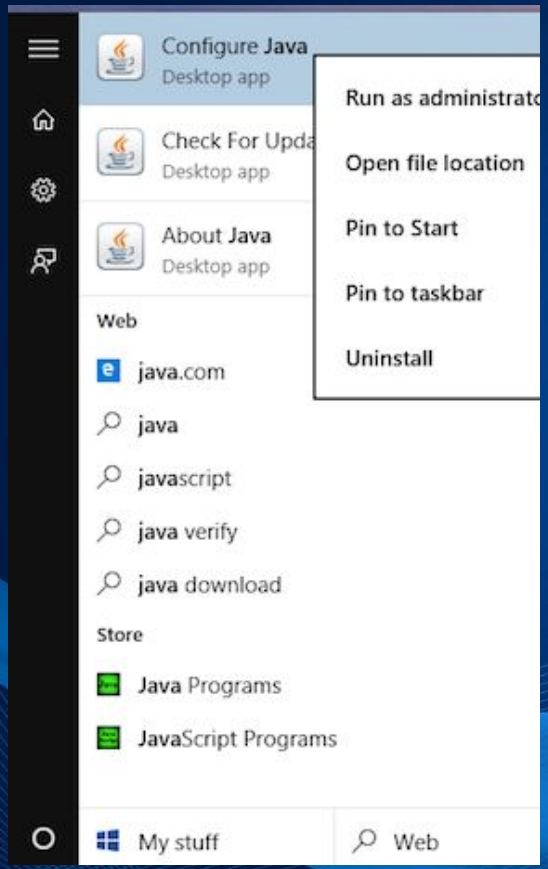


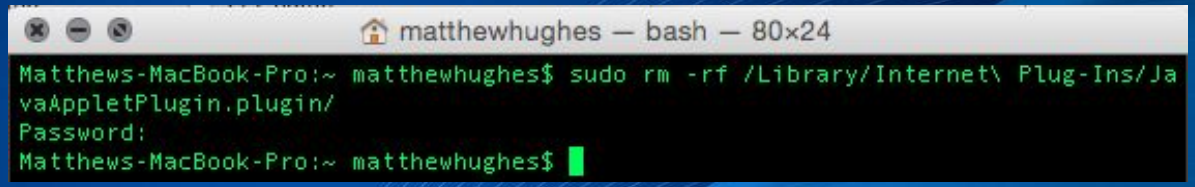
- **FTC demanded Oracle to post a formal letter on their official website for 2 years, to inform all customers of their Java insecurities**

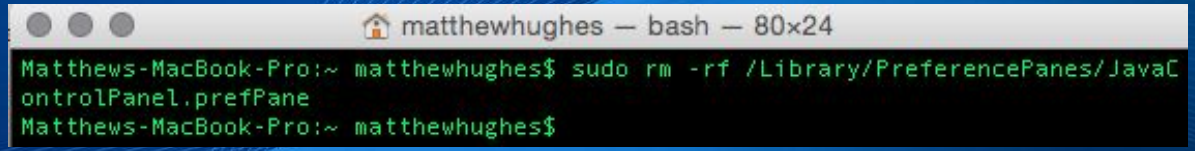
How do you protect yourself from cyber threats targeting Java?

- Software updates – just do them!
- Use a strong antivirus
- Use a security tool that can block advanced malware
- Secure your browsers!

Remove Java!


Configure Java
Desktop app
Check For Upda
Desktop app
About Java
Desktop app
Run as administrato
Open file location
Pin to Start
Pin to taskbar
Uninstall
Web
java.com
java
javascript
java verify
java download
Store
Java Programs
JavaScript Programs
My stuff
Web


matthewhughes — bash — 80×24
Matthews-MacBook-Pro:~ matthewhughes$ sudo rm -rf /Library/Internet\ Plug-Ins/JavaAppletPlugin.plugin/
Password:
Matthews-MacBook-Pro:~ matthewhughes$


matthewhughes — bash — 80×24
Matthews-MacBook-Pro:~ matthewhughes$ sudo rm -rf /Library/PreferencePanes/JavaControlPanel.prefPane
Matthews-MacBook-Pro:~ matthewhughes$

Moving to a Plugin-Free Web

- Browsers to discontinue support for NPAPI (Netscape Platform API), no more Java applets!
- Also includes: Adobe's Flash , Silverlight, Unity, and the Facebook plugins

Browsers that no longer support Java

- Google Chrome
- Windows 10 Edge
- Mozilla Firefox (by end of the year)

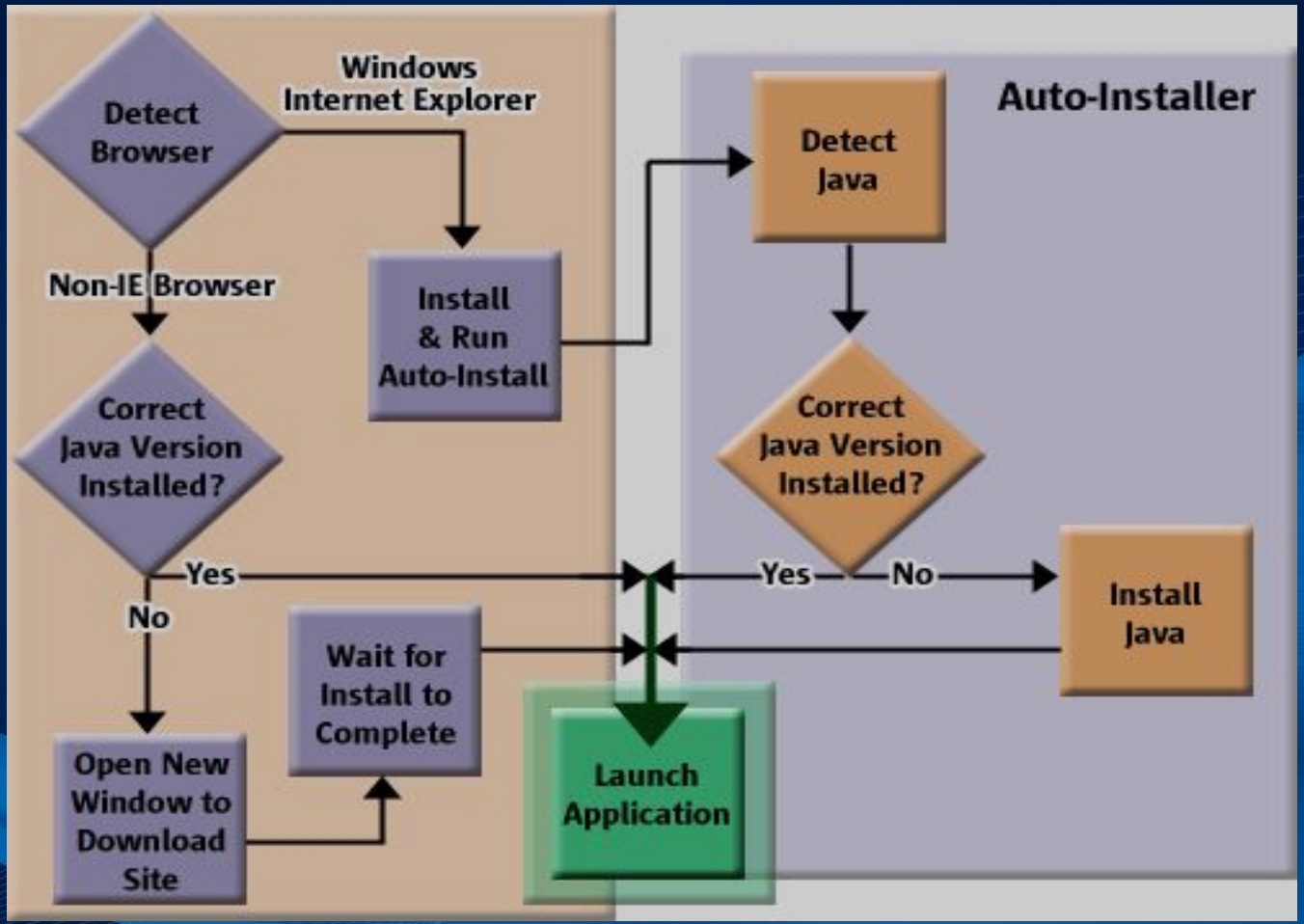
Oracle will also be deprecating the java browser plugin in its JDK 9 release in September.

Oracle to replace it with Java Web Start technology.

What is Java Web Start (JAWS) Technology?

The Java Web Start software allows you to download and run Java applications from the web. The Java Web Start software:

- Provides an easy, one-click activation of applications
- Guarantees that you are always running the latest version of the application
- Eliminates complicated installation or upgrade procedures


Detect Browser
Windows Internet Explorer
Non-IE Browser
Install & Run Auto-Install
Auto-Installer
Detect Java
Correct Java Version Installed?
Correct Java Version Installed?
Yes
No
Yes
No
Install Java
Wait for Install to Complete
Open New Window to Download Site
Launch Application

Discussion questions

1. Keeping Java plugins up to date is a good idea, but what is the best thing to do to ensure your system is safe?

   Remove the plugins completely, and use plugin-free browsers or JAWS.

2. What is used to exploit Java's vulnerabilities?

   Exploit Kits

3. Why would an exploited vulnerability be undetectable by a user?

   The user does not give any authorization

References

https://heimdalsecurity.com/blog/java-biggest-security-hole-your-computer/

http://www.makeuseof.com/tag/web-just-became-secure-google-drops-support-java/

http://thehackernews.com/2015/12/java-insecure-hacking.html

http://www.theregister.co.uk/2015/12/22/ftc_oracle_java/

http://www.oracle.com/technetwork/systems/index-155997.html

https://heimdalsecurity.com/blog/ultimate-guide-angler-exploit-kit-non-technical-people/

http://www.asd.gov.au/publications/protect/minimising_java_threats.htm

https://blogs.oracle.com/java-platform-group/entry/moving_to_a_plugin_free

http://www.howtogeek.com/179213/why-browser-plug-ins-are-going-away-and-whats-replacing-them/

References

https://blog.malwarebytes.org/intelligence/2013/02/tools-of-the-trade-exploit-kits/

https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/