Stagefright! Dangerous Times, and Welcome Improvements

Joshua Wright
@joswr1ght
jwright@willhackforsushi.com

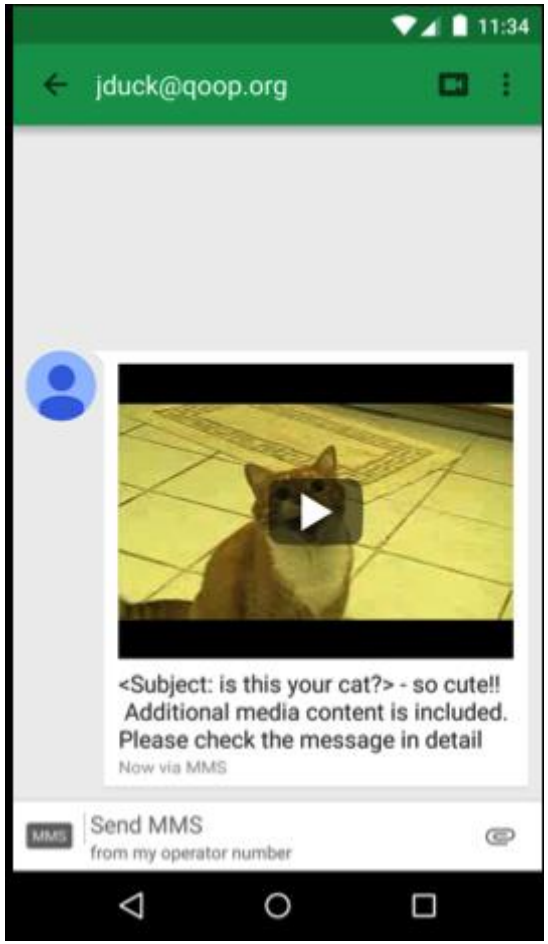
Introduction

- Overview of the Stagefright vulnerability
- Detecting vulnerable devices
- Stagefright countermeasures, patching status
- Reflections on the Android ecosystem
- Practical advice for responding to Stagefright

SANS Webcasts: Bringing you what you need to know without scouring through hundreds of random blogs and tweets.

Stagefright Overview

- Several vulnerabilities identified by Josh Drake (@jduck) of Zimperium
  - CVE-2015-1538, CVE-2015-1538, CVE-2015-1538, CVE-2015-1538, CVE-2015-1539, CVE-2015-3827, CVE-2015-3826, CVE-2015-3828, CVE-2015-3824, CVE-2015-3829
- Multiple buffer overflow vulnerabilities in the Android stagefright media library
  - Triggered when handling crafted MP4 files
- Affects all Android devices from Android 2.2 to 5.1.1
  - Estimated 950M vulnerable Android users



Stagefright Delivery Vector

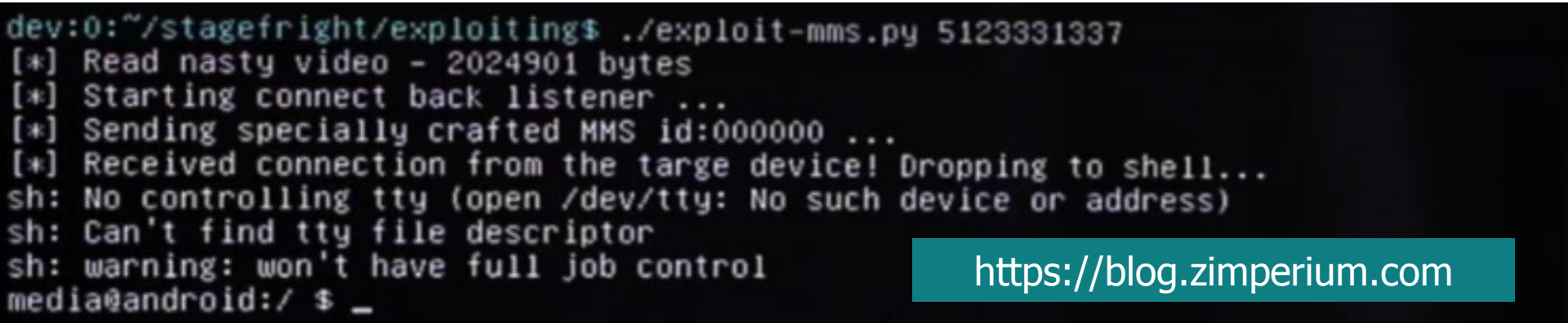
- Videos carrying exploit can be delivered over MMS
- Affects default MMS applications and third-party MMS (Google Hangout, et. al.)
- Exploit can also be delivered through more traditional vectors
  - Including malicious web pages or email attachments

```
<video autoplay>
  <source src="stagefrightex.mp4" type="video/mp4">
</video>
```

Even tablet devices with no MMS feature are vulnerable

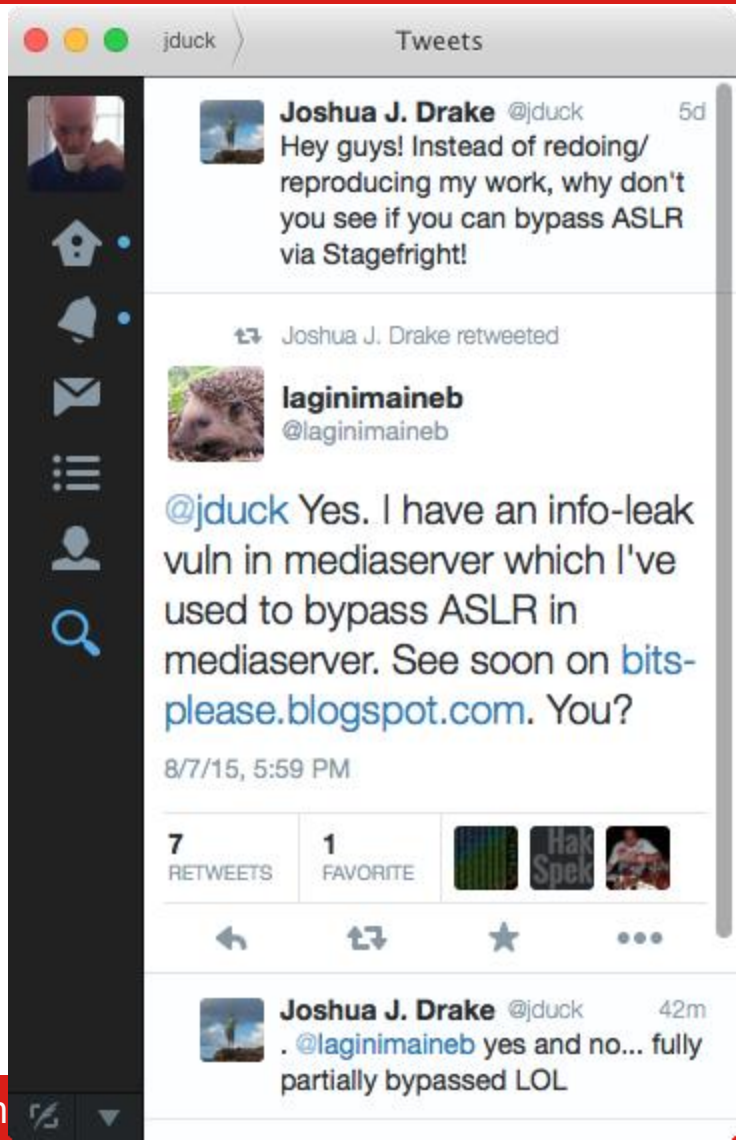
Practical Exploitation: What We Know

- Drake has released proof-of-concept crash MP4s, no exploit code
  - Also posted a video exploiting an Android phone
- Commercial VulnDisco exploit pack for ImmunitySec CANVAS tool claims support
- Android 4.1 and later has ASLR support, making exploitation more difficult
  - Android <4.1 users have a lot more problems than Stagefright to worry about (9% of devices)

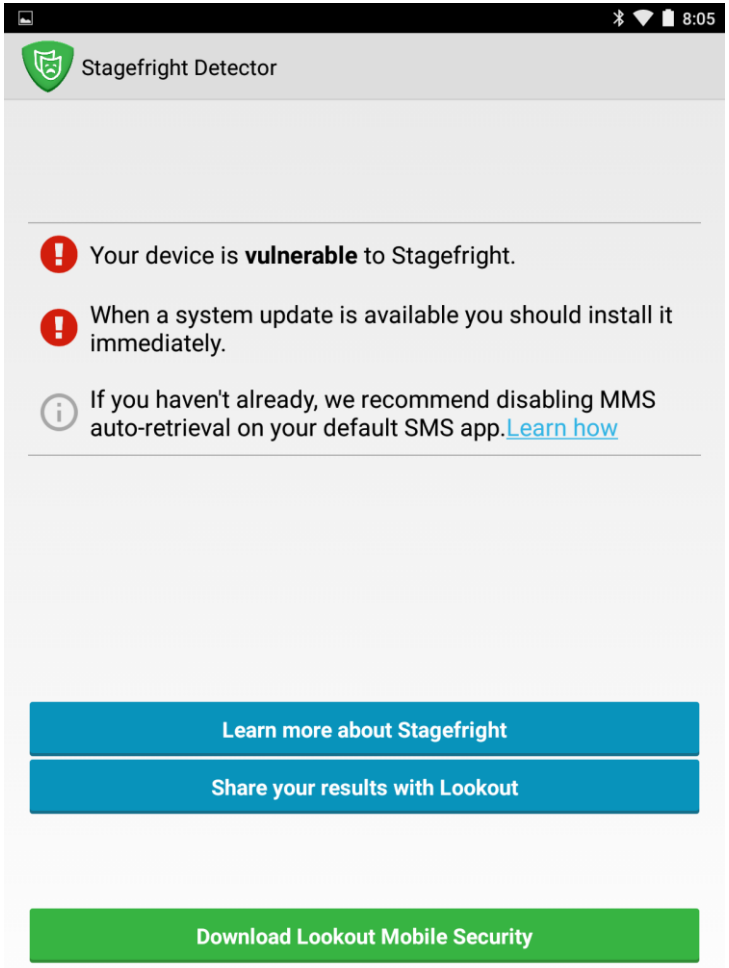


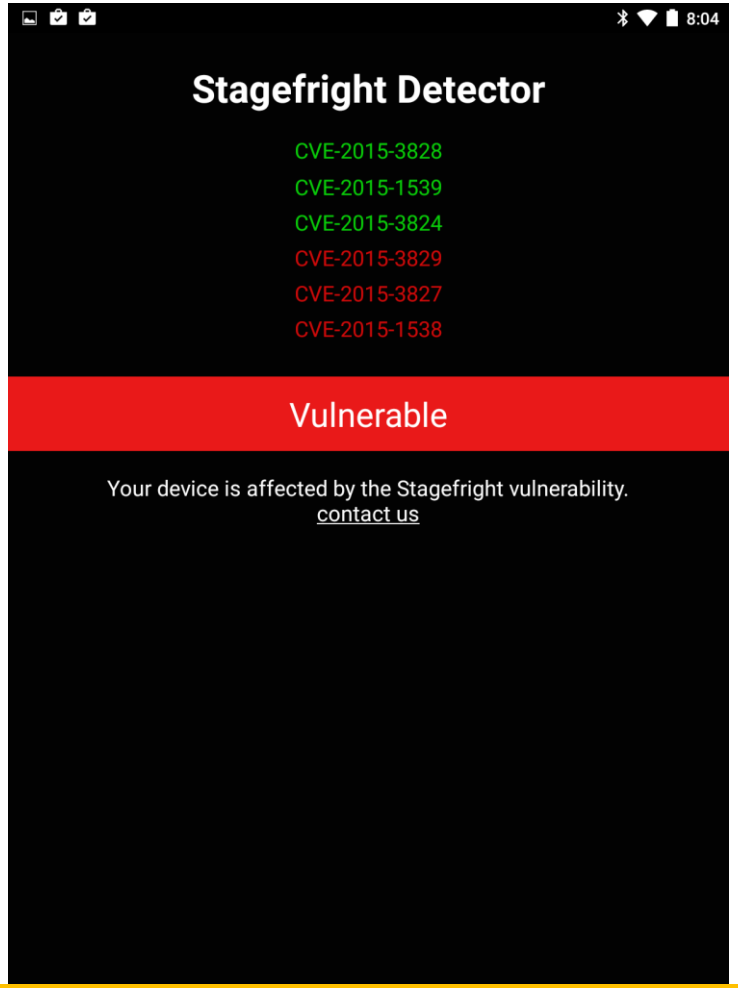
What We Also Know

- Zimperium will release their exploit on 8/24 for testing purposes
  - Unless another exploit in the wild is observed first, then immediately
- People are working on exploits, and reliable ASLR bypass



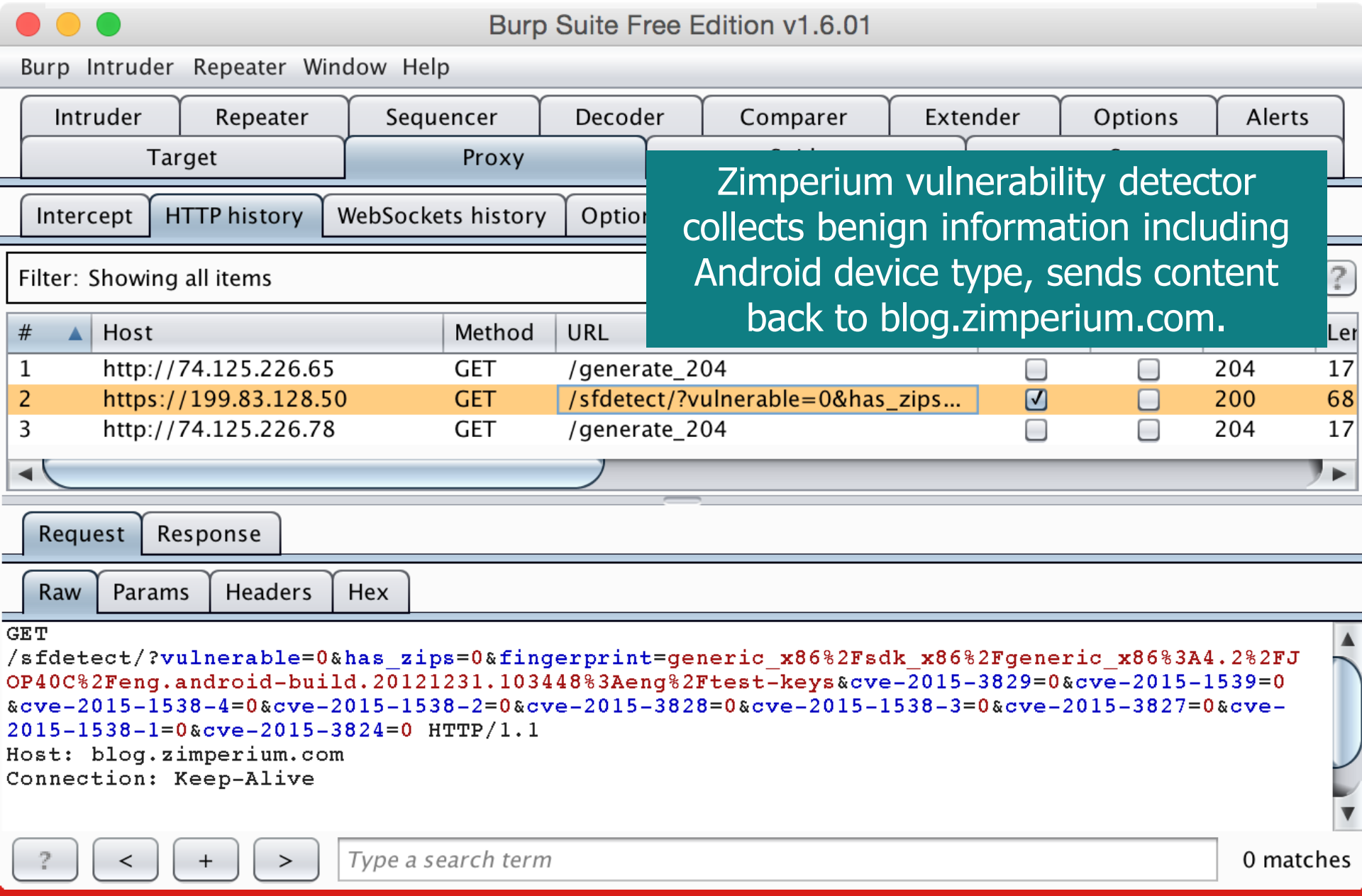
Vulnerability Detection





Apps from Lookout Mobile and Zimperium both detect vulnerable devices. Available in the Google Play Store.

Data Harvesting



Zimperium vulnerability detector collects benign information including Android device type, sends content back to blog.zimperium.com.

Countermeasures

- Disable auto-retrieval of MMS messages
  - Allows user to manually retrieve messages from trusted sources
  - Doesn't defend against browser delivery vector
  - Doesn't help if known user gets compromised, and his contact book is used to identify new victims
- Instructions for disabling auto-retrieval varies across different messaging platforms
  - Messages, Messaging, Messenger, Hangouts

https://blog.lookout.com/blog/2015/07/28/stagefright/

Patch Status

- Samsung, HTC, LG, Sony, Motorola and Android One have announced patches or plans to patch
  - Status from ZTE, Kyocera, and other handset manufacturers is unclear
- Third-party ROM provider Cyanogenmod v12.1 nightly builds are patched

Some handset manufacturers are already releasing patches to resolve the vulnerability. If and when users will get these patches remains unknown.

The Bottom Line

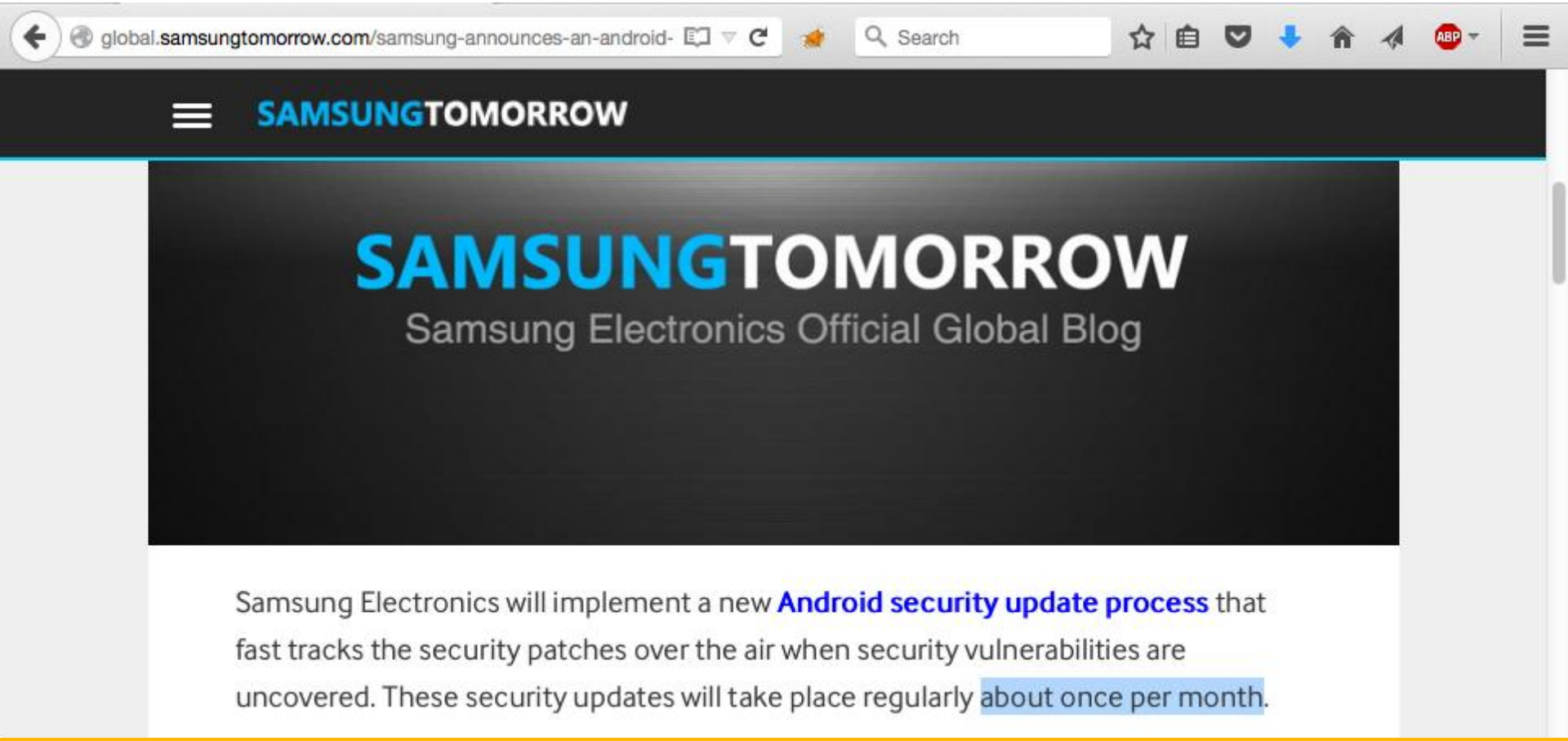
- Many millions of Android users will be vulnerable for many years to come
- Android JellyBean (4.1-4.3) has been abandoned from a vendor support perspective
  - Last updated 7/2013
  - 30.1% Android users
  - About 286 million devices (assumes 1B total)
  - No patches. No support. Nada. Buy a new phone.

This has led me to arrive at two conclusions.

The Android Security Model is Broken.

Stagefright is the best thing that has happened to Android users.

The Good News!



Google, Samsung, and LG pledged to make monthly security updates available.

This is really good news, right?

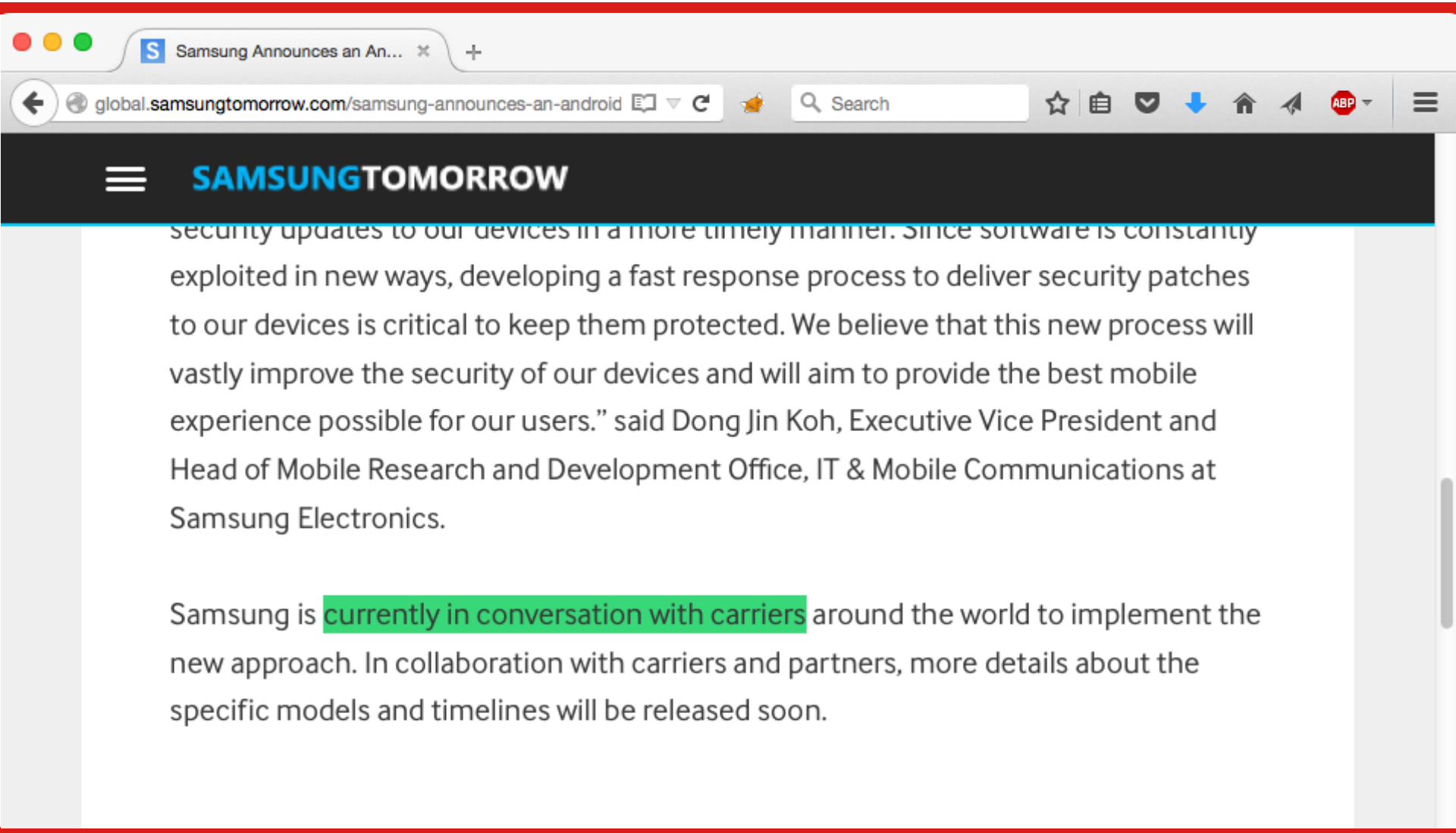
It is Awesome News

- Handset manufacturers are moving to 21st century patching policies
- This would not have happened without a stagefright-class exploit and media
- Customers should consider this benefit when buying phones

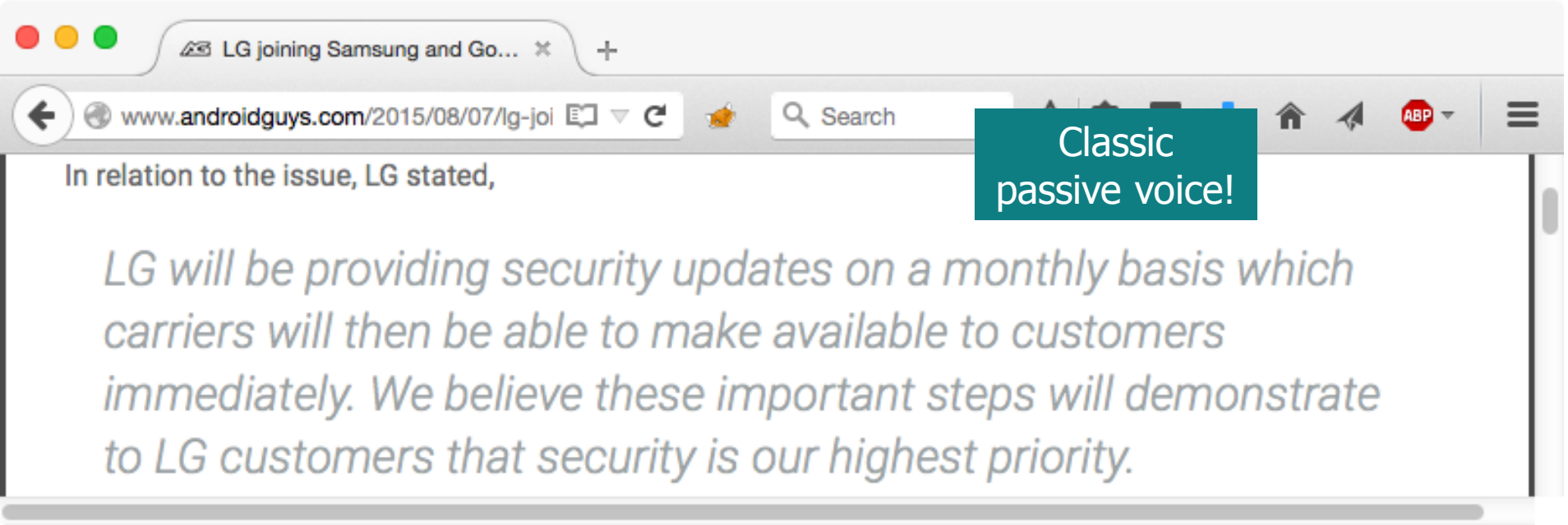
Why would I buy a phone from HTC, Android One, Sony, Kyocera, ZTE, or Motorola if they can't commit to supporting me with regular security updates?

Sadly, not everything is rosy with LG and Samsung

Mobile Operator Woes

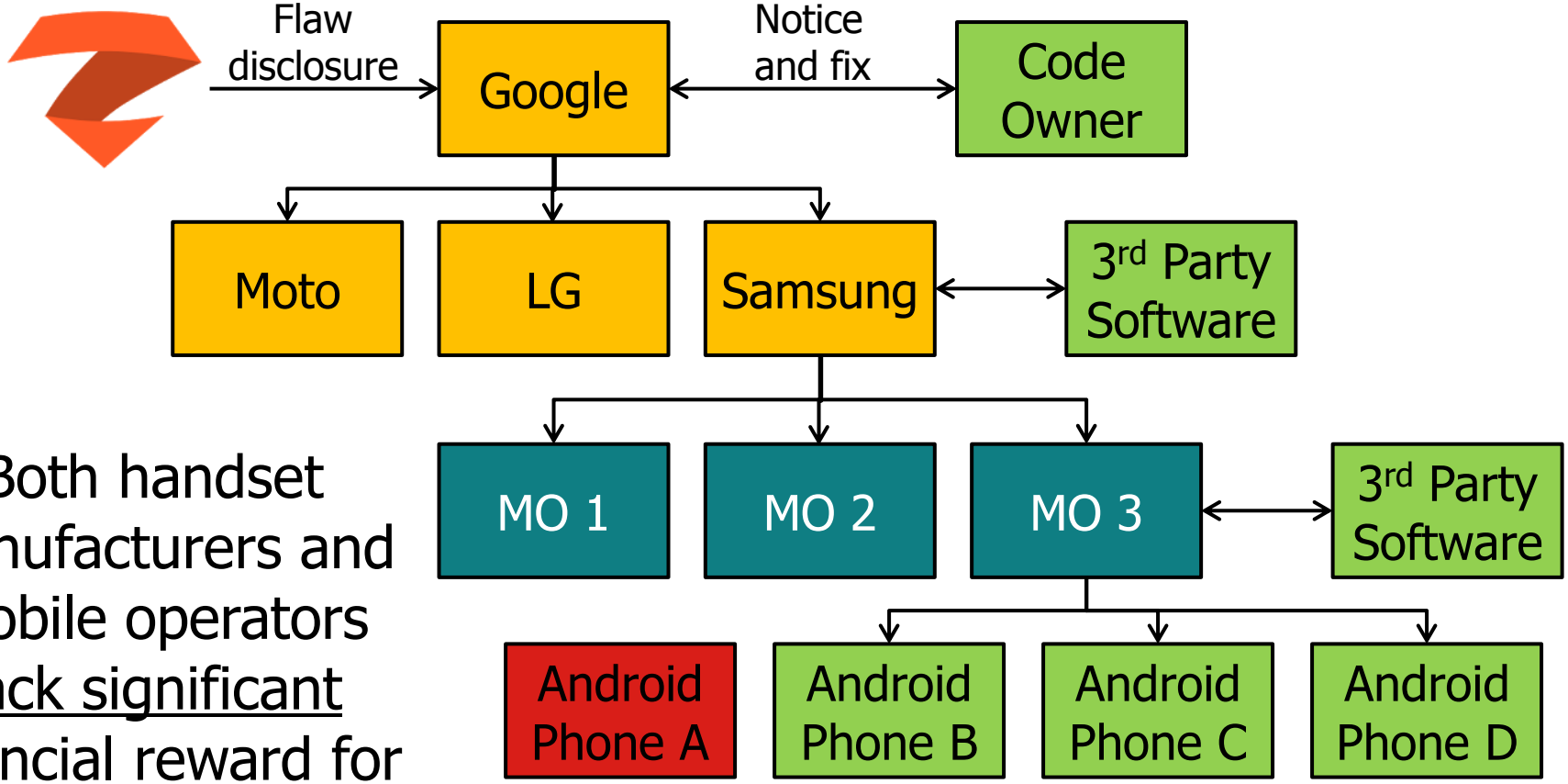


LG and Motorola Statements



I welcome these handset manufacturers to patch management in the 21st century, but they lack the total ownership of patch delivery. Carriers stand between you and the patches you need.

Android Security Fix Process



Both handset manufacturers and mobile operators lack significant financial reward for continued support of Android devices.

Updates to fix the Stagefright exploit are beginning to roll out from Sprint, and now AT&T is joining with updates for a bunch of Samsung phones. The update, which includes a 'device security enhancement' is now pushing out from the carrier. The update is currently showing as available for the following devices:

- Samsung Galaxy Note 4
- Samsung Galaxy S6
- Samsung Galaxy S6 edge
- Samsung Galaxy S6 Active
- Samsung Galaxy S5

My shining ray of hope is ... AT&T?

Practical Patching

- AT&T and Sprint are making updates available for limited devices
  - Focusing on devices solid within the last 14 months (Samsung Galaxy S5 and later)
- Google is distributing updates for Nexus users directly
  - Google does not have to coordinate with carriers, since they don't accept carrier software add-ons

We will have to wait and see what other mobile operators offer for patches as more handset manufacturers make the patches available.

What to Do

- Users should contact their mobile operators to ask for patches
  - Repeatedly, and often
- Users should consider the support they get from their handset manufacturer
  - And take that support into consideration when it's time to buy a new device
- Users should strongly consider buying Nexus devices

Nexus devices eliminate the carrier for software updates, with integrated support right from Google. Updates with Nexus are almost as good as ...

Apple iOS

- iPhone 4S
- Introduced October, 2011
- Still supported today with iOS 8.4

Apple has a strong financial motive to continue supporting older devices with updates (30% of everything in the App Store). Best available support and software update availability for smartphones.

Conclusion

- Stagefright is a considerable threat to many Android devices
  - Mitigated by platform security controls on modern devices (today)
- Apps from Lookout, Zimperium detect the threat
- Disabling MMS is difficult with various MMS apps available for Android users
  - Also, traditional exploit vector through web delivery
- Android is amazing, but patching is broken
  - Some progress from vendors, but users need to demand support from carriers with their buying power

www.sans.org/webcasts/archive
www.willhackforsushi.com/presentations/stagefright.pdf