Security Now! #524 - 09-08-15

Q&A #218

Leo… hearing aid??
Podcast's Audio Quality

This week on Security Now!

- Seagate WiFi Drive Nightmare.
- AdBlock plus releases Adblocking browsers on the eve of iOS 9.
- Are Chrome & YouTube blocking blockers?
- Android phones now coming with pre-installed Malware.
- Update on Click-to-Play options.

A hard drive's multiple glass platters shattered

Security News:

Seagate's WiFi Drive Nightmare

- https://www.tangiblesecurity.com/index.php/announcements/tangible-security-researchers-notified-and-assisted-seagate-with-fixing-critical-device-vulnerabilities
- The following devices with firmware versions 2.2.0.005 and 2.3.0.014, dating to October 2014, are vulnerable to three attack vectors (below). Other firmware versions may be affected.
    - Seagate Wireless Plus Mobile Storage
    - Seagate Wireless Mobile Storage
    - LaCie FUEL
    - (Perhaps others under various OEM rebranding)
- Use of Hard-coded Credentials
    - The affected device firmware contains undocumented Telnet services accessible by using the default credentials of 'root' as username and the default password.
    - An attacker can covertly take control of the device, not only compromising the confidentiality of files stored on it, but use it as a platform to conduct malicious operations beyond the device.
- Direct Request ('Forced Browsing')
    - The affected device firmware provides unrestricted file download capability.
    - Attackers can gain access to all files stored in affected devices. This vulnerability requires attackers to be within range of the device's wireless network.
- Unrestricted Upload of File with Dangerous Type
    - The affected device firmware provides a file upload capability to the device's /media/sda2 file system, which is reserved for file sharing.
    - This vulnerability requires attackers to be within range of the device's wireless network, who can upload files onto it. If such files were maliciously crafted, they could compromise other endpoints when the files are opened.
- Timeline:
    - Seagate notified on March 18th, 2015.
    - Seagate confirms vulnerabilities on March 30th (12 days).
    - Tangible Security tests & confirms patch. (~100 days).
- https://apps1.seagate.com/downloads/request.html

AdBlock Plus Browser -- Alternative Mobile Web Browser for Android and iOS

- "AdBlock Browser" - from the App Store & the Google Play store.
    - Careful: get the one by "Eyeo"
    - Logo: Portion of a stopsign covering aa portion of the world.
        - A bit like the globe is wearing a jaunty hat.
- https://adblockplus.org/blog/first-official-ad-blocker-for-ios-launches-today-ditto-for-android
- "First official ad blocker for iOS launches today; ditto for Android"
- "Adblock Plus beats iOS 9 to App Store; returns from exile to Play Store"
    - March 14th - EFF - "Google Takes the Dark Path, Censors AdBlock Plus on Android"
    - https://www.eff.org/deeplinks/2013/03/google-censoring-android-apps
    - "In a shocking move, Google has recently deleted AdBlock Plus from the Android

Play Store. This is hugely disappointing because it demonstrates that Google is willing to censor software and abandon its support for open platforms as soon as there's an ad-related business reason for doing so."
    - "Google's stated reason for the ban is that the Android app allegedly "interferes with or accesses another service or product in an unauthorized manner."
- "Why wait a few weeks to block ads in Safari? Adblock Browser is here today."
- Features:
    - Adblocking via EasyList
    - "More Blocking Options" (all OFF unless turned ON)
        - Disable Tracking (ON)
        - Disable Malware Domains (ON)
        - Disable Social Media Buttons (ON)
        - Disable Anti-Ad blocking Messages (-off-)
    - Acceptable Ads
        - "Allow some non-intrusive ads"
    - Whitelisted Domains
        - …

Reports of YouTube preventing Ad blocking pre-reroll commercial skipping appear specious

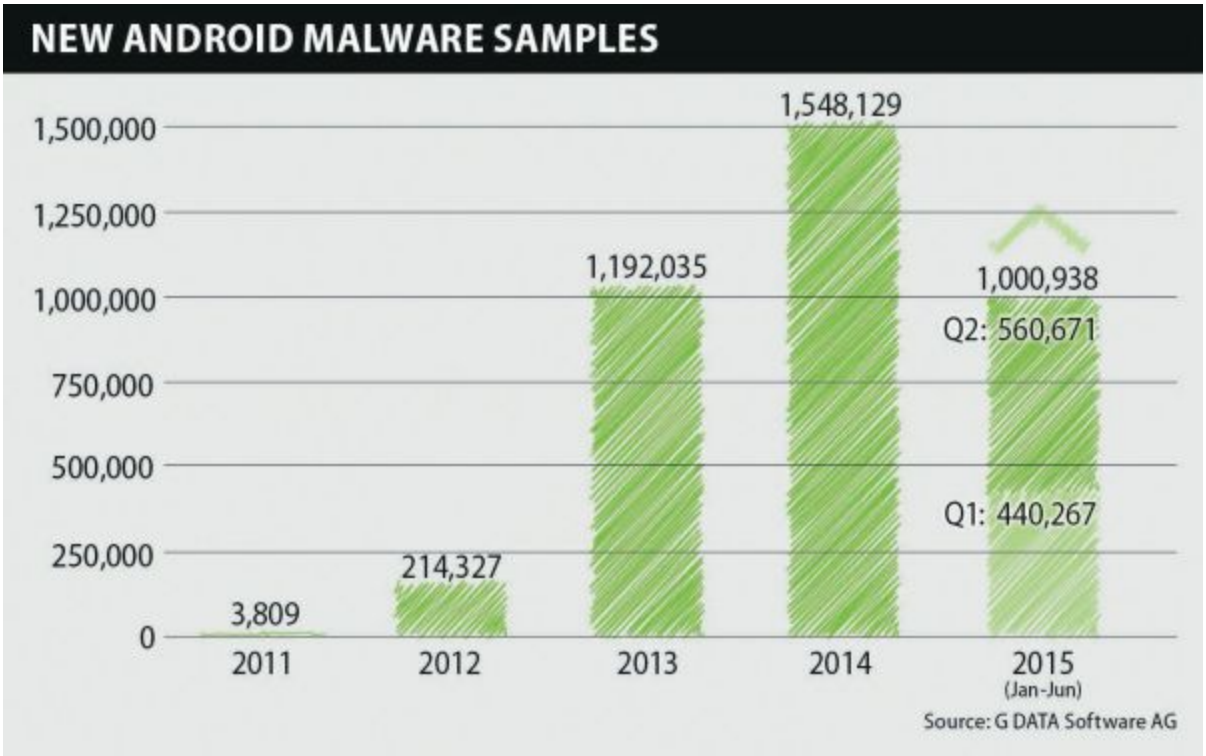
- It was a side-effect of a non-public security fix.
- It affected all ad blockers by not calling "chrome.webRequest.onBeforeRequest()" for registered extensions.
- It's getting fixed:
    - Issue 510802: Security: webRequest API allows intercepting XHR from apps and extensions
    - VULNERABILITY DETAILS
        - webRequest API allows extensions to intercept and redirect requests from the browser. That includes requests from other extensions.
        - However, it also allows to intercept XMLHttpRequest requests from Chrome Apps, which is quite possibly unintended. Chrome Apps are supposed to be as much independent from the browser as possible.

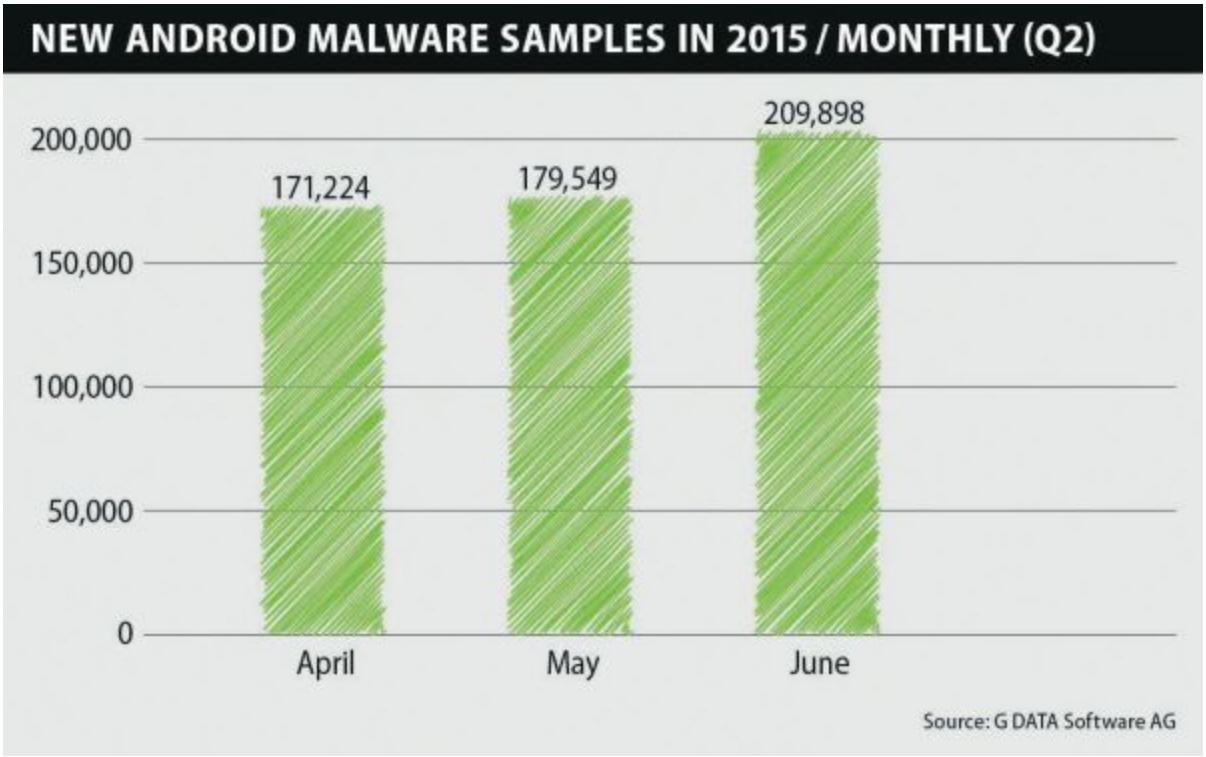
Malware found Pre-Installed on Huawei, Xiaomi and Lenovo phones.

- http://au.idigitaltimes.com/malware-found-pre-installed-xiaomi-huawei-lenovo-phones-107190
- German-based cyber security firm, G Data, has seen a 25 percent increase in pre-installed malware during the past six months.
- Apps are modified to spy on its users and/or insert ads.
- Malware appears to be firmware-based so that removing the application doesn't help.
- The Facebook and Google Drive apps are infected on the fly when installed on the phone.
- Christian Lueg, the spokesperson for G Data, explained that the malware was injected by a middleman. The security firm tried to backtrack its source and immediately traced it back to China, but that is the farthest the researchers have reached. "We lost the trail in China," he stated.
- 26 smartphone units were discovered to be carrying malicious software before the consumer acquires the device.
- Devices infected with this firmware malware: Xiaomi Mi 3, Huawei G510, Lenovo S860, Alps A24, Alps 809T, Alps H9001, Alps 2206, Alps PrimuxZeta, Alps N3, Alps ZP100, Alps

709, Alps GQ2002, Alps N9389, Android P8, ConCorde SmartPhone6500, DJC touchtalk, ITOUCH, NoName S806i, SESONN N9500, SESONN P8, Xido X1111

- The trouble appears to be 3rd-party middlemen suppliers.
- Never use unofficial channels. Only buy direct from major suppliers.
- https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q2_2015_EN.pdf





Click-to-play Update

- Heard back from many who changed their settings in Chrome.
  - chrome://settings/content
  - "Let me choose when to run plugin content"
- Mozilla:
  - Tools / Add-ons / Plugins
  - "Ask to Activate:

SpinRite:

Quinton in Nova Scotia, Canada
Subject: How do you test SpinRite?

With the mentions of SpinRite on the last few episodes of Security Now, it got me thinking about how you actually go about developing SpinRite itself. More specifically, how do you actually test SpinRite? How do you know that it is detecting an error on the hard drive and it's not just an error in your code?

I'm imagining there are two different ends of the spectrum of how it is possible to know exactly where the problems are on a drive for testing and verifying your code. On one side you are cracking open a hard drive, putting it under a microscope, counting the sectors and bits and strategically destroying some data so that you know exactly where the drive will fail.

On the other side you have a virtualized hard drive where you are able to corrupt bits at your leisure.

How exactly do you go about this? I'd love to hear your thoughts on the next episode of Security Now.

Thanks