Security Now! #544 - 01-26-16

Q&A #228

This week on Security Now!

- More on the consumer encryption fight
- A smartphone updating lawsuit
- A new web compression standard
- A website that (deliberately) crashes iOS
- A new Firefox
- A bit of Miscellany and ten comments, questions or tips from our great followers!

Security News:

Another bill (Wednesday) seeks to weaken encryption-by-default on smartphones
http://arstechnica.com/tech-policy/2016/01/yet-another-bill-seeks-to-weaken-encryption-by-default-on-smartphones/

CA Asm. Jim Cooper: "Human trafficking trumps privacy, no ifs, ands, or buts about it."

[Ars] A second state lawmaker has now introduced a bill that would prohibit the sale of smartphones with unbreakable encryption. Except this time, despite very similar language to a pending New York bill, the stated rationale is to fight human trafficking, rather than terrorism.

Specifically, California Democratic Assembly member Jim Cooper's new bill, introduced last Wednesday, would "require a smartphone that is manufactured on or after January 1, 2017, and sold in California, to be capable of being decrypted and unlocked by its manufacturer or its operating system provider."

In a phone interview with Ars, Jim Cooper, a 30 year veteran of the Sacramento County Sheriff's Department said: "If you're a bad guy, [law enforcement] can get a search record for your bank, for your house, you can get a search warrant for just about anything. For the industry to say it's privacy, it really doesn't hold any water. We're going after human traffickers and people who are doing bad and evil things. Human trafficking trumps privacy, no ifs, ands, or buts about it."

Samsung sued by the Dutch Consumer's Association (DCA)
... over its failure to patch vulnerable consumer smartphones.

Last year's "Stagefright" vulnerabilities highlighted the fundamental problem:

- Smartphones are more computers than phones and, as such, they will be rampant with vulnerabilities that will only be discovered over time.
- They will also be filled with private data.
- Therefore... they MUST HAVE an update mechanism as part of their package.

According to DCA's own research, at least 82 percent of Samsung smartphones available in the Dutch market examined had not received any software updates on the latest Android version in two years. This failure to provide software updates left the majority of Android devices vulnerable to issues on security and others. The DCA says that the agency has previously contacted Samsung many times and discussed the matter privately with the manufacturer giant to resolve the situation, but it failed to reach an agreement with the company, and so it decided to go to court.

While the more recent high-end Samsung Galaxy S6 series may have received Stagefright patches, Samsung has failed to provide Stagefright fixes for its majority of midrange and entry-level Android devices. And none of Samsung's devices currently runs the latest Android 6.0 Marshmallow, three months after it officially launched.

What the DCA wants:

- The agency is demanding that Samsung update all of its smartphone devices to the latest version of Android operating system for two years from the handset's purchased, not its launch.
- The agency wants Samsung to treat software updates as part of the warranty that has its length mandated at two years in the European Union.
- "[We are] demanding that Samsung provides its customers with clear and unambiguous information about this," The DCA writes. "Also, [we are] demanding that Samsung actually provides its smartphones with updates."

Google's next-generation GZIP replacement "Brotli" moves to "intent to ship" status
Brotli?
Sept 22 20155:
http://google-opensource.blogspot.co.uk/2015/09/introducing-brotli-new-compression.html
At Google, we think that internet users' time is valuable, and that they shouldn't have to wait long for a web page to load. Because fast is better than slow, two years ago we published the Zopfli compression algorithm. This received such positive feedback in the industry that it has

been integrated into many compression solutions, ranging from PNG optimizers to preprocessing web content. Based on its use and other modern compression needs, such as web font compression, today we are excited to announce that we have developed and open sourced a new algorithm, the Brotli compression algorithm.

While Zopfli is Deflate-compatible, Brotli is a whole new data format. This new format allows us to get 20–26% higher compression ratios over Zopfli. In our study 'Comparison of Brotli, Deflate, Zopfli, LZMA, LZHAM and Bzip2 Compression Algorithms' we show that Brotli is roughly as fast as zlib's Deflate implementation. At the same time, it compresses slightly more densely than LZMA and bzip2 on the Canterbury corpus. The higher data density is achieved by a 2nd order context modeling, re-use of entropy codes, larger memory window of past data and joint distribution codes.

As with Zopfli, the new algorithm is named after Swiss bakery products. Brötli means 'small bread' in Swiss German.

The smaller compressed size allows for better space utilization and faster page loads. We hope that this format will be supported by major browsers in the near future, as the smaller compressed size would give additional benefits to mobile users, such as lower data transfer fees and reduced battery use.
http://www.gstatic.com/b/brotlidocs/brotli-2015-09-22.pdf

- Accept-Encoding: br
- ONLY over https connections
- Brotli outperforms gzip for typical web assets (e.g. css, html, js) by 17–25 %.
    - Brotli -11 density compared to gzip -9:
    - html (multi-language corpus): 25 % savings
    - js (alexa top 10k): 17 % savings
    - minified js (alexa top 10k): 17 % savings
    - css (alexa top 10k): 20 % savings

Status:

- The Brotli spec has been independently reviewed and implemented by Mark Adler.
- Developer interest is high: interest from CDN vendors, tier1 web properties, third parties, nginx modules (cloudflare, google)...
- Brotli has been in use in WOFF2 (Web Open Font Format v2) web fonts for a while with no compatibility issues.
- Supporting Brotli for content-encoding is rather straightforward when you already support WOFF2
- WOFF2 is supported in Chrome, Opera, Firefox

- support for WOFF2 in Safari has recently landed (My read of webkit#150830)
- support for WOFF2 is under consideration for Edge.
- Brotli is supported by Firefox since M44 (also restricted to HTTPS connections)
- Brotli is under consideration by the Edge team (pending pull request by Kyle Pflug, Edge program manager)
- Brotli support in Safari: no public signals other than upcoming WOFF2 support (with Brotli under the hood)

Stay away from: http://crashsafari.com/

- Venture Beat, Engadget, 9to5mac, techcrunch, BGR...
- A new prank circulating on Twitter, Facebook, etc.
- Crashes iOS/Safari devices. -- Actually CRASHES the OS!
- My Firefox needed a restart.
- Android not immune either.
- People are spreading it as ClickBait via Twitter with a link shortener.
- What is it?
    - HTML5 History API
    - var total = "";
      for(var i=0; i<100000; i++) {
        total = total + i.toString();
        history.pushstate(0,0,total);
      }
- The History interface allows the manipulation of the browser session history: The history of the pages visited in the tab or frame that the current page is loaded in.
- The HTML5 History API is slow... so it takes longer to maintain the list than it takes new entries to come in. It becomes too much, and it tanks.
- A small piece of JavaScript that calls the HTML5 History API thousands of times in a loop, potentially causing Safari to freeze.
- Known of since 2014.

Crashsafari was created by Matthew Bryant, a 22-year-old working in application security in San Francisco.
Matthew said to Wired: “In my spare time I often test how browsers will handle odd code that gets thrown at them.”
He stumbled on the bug independently, made the browser- and phone-crashing sites "purely as a joke."

Firefox v44 released today

- Windows, Mac, Linux, and Android.
- Push notifications
  - Added in Chrome 42 last April.
  - "Would you like to receive notifications from this site?"
- RC4 completely removed
  - Last week's Chrome 48 also dropped support.
- New web page authoring tools
- Improved warning pages for certificate errors and untrusted connections
- Enable H.264 if system decoder is available
- Enable WebM/VP9 video support on systems that don't support MP4/H.264
- Support the brotli compression format via HTTPS content-encoding
- Various security fixes
- Firefox will no longer trust the Equifax Secure Certificate Authority 1024-bit root certificate or the UTN – DATACorp SGC to validate secure website certificates
- New memory tool for inspecting the memory heap
- Built-in JSON reader to intuitively view, search, copy and save data without extensions

Miscellany

The Expanse (tonight!)

- My reply to a Titter comment:
- Peter…
  I have NO IDEA how they are making it so good, and I agree, it has become absolutely fantastic! And, since I've read the books... just WAIT for this week's episode! <g> We get to see the first real hint about the MUCH MUCH MUCH MUCH bigger thing that's actually going on! <<grin>>
- Reminiscent of Firefly.
- Just WAIT until tonight!!! <g>

- Ben Roberts (@broberts76)
  @SGgrc Thanks!! Glad you're enjoying the show!! #TheExpanse
  Ben: Senior VP of TV w/Alcon Entertainment.
  Producing THE EXPANSE, ICE, SINATRA (HBO) and many more coming soon!!
  Formerly developed AMC's THE WALKING DEAD!

SpinRite

David White
Location: Auckland, New Zealand
Subject: SpinRite Success Story
:
Hi Steve,

A quick SpinRite story for you.

I bought a copy of SpinRite from you about 2 months ago, not because I needed it at the time, but just to give you a 'yabba dabba doo' in appreciation for the SN podcast, which I listen to religiously every week. (I'm also filling in my drive time by starting at episode one again).

I am a freelance IT guy in Auckland, New Zealand, and look after IT needs for a number of small businesses. This morning I heard my cell phone ringing before I had even gotten out of bed – never a good sign! It was a customer whose main Windows 7 PC (the one with their shared files and database on it) was getting stuck on the welcome screen immediately after logon. Once I got to their site, I was able to boot it into safe mode and attempted a system restore, which failed with an error indicating a problem with the drives volume shadow copy. I tried it a second time, and this time got a BSOD.

I booted back into safe mode, and ran chkdsk /r – 40 minutes later it reported that there were no problems on the disk, but my gut was telling me otherwise. I unplugged the PC , took it back to my office and booted it up with my SpinRite disk. Three hours later, I was on my way back to the customer with a fully working PC on the back seat.

The customer was of course delighted, so thanks a million for making me look good!

One last thing – it may be my over excited imagination, but I swear that PC ran faster after the SpinRite repair than it ever had since I installed it 5 years ago.

Thanks again,
Regards
David