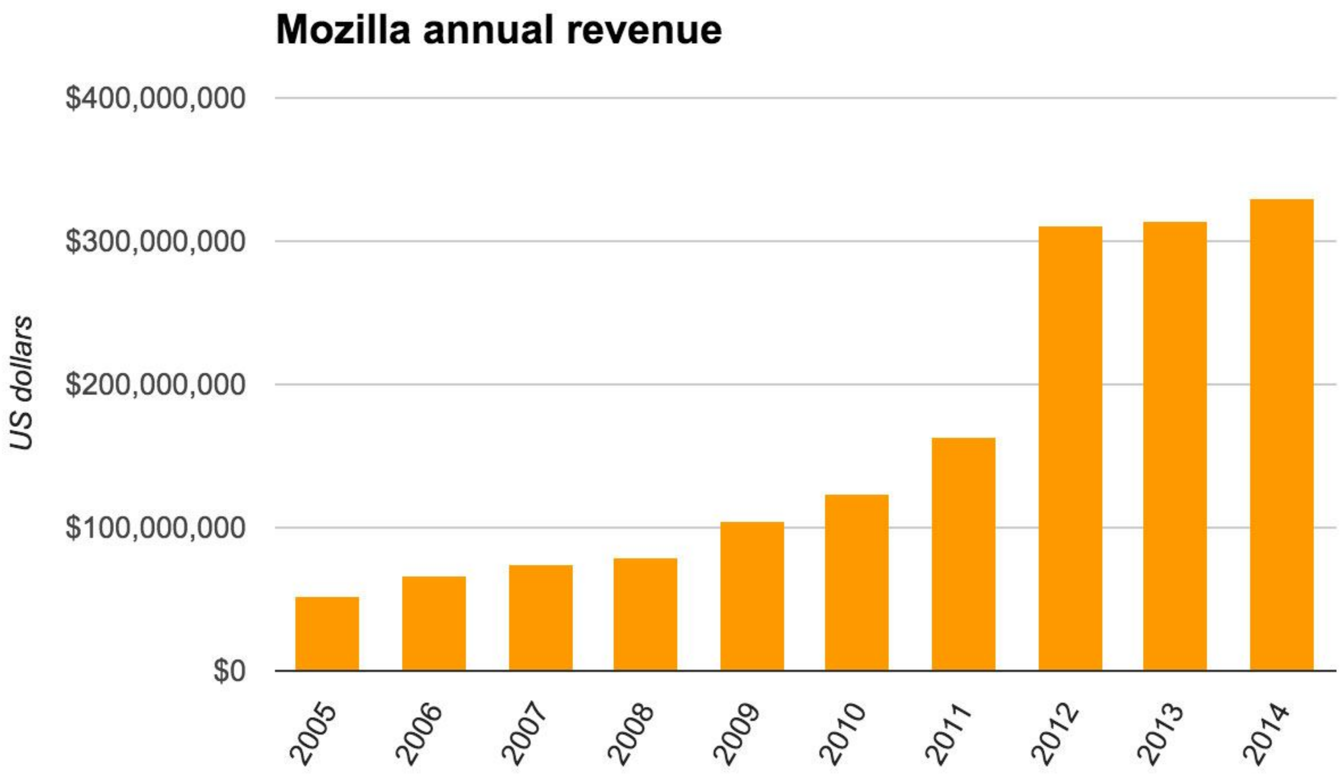
Security Now! #536 - 12-01-15

Listener Feedback, Q&A #224

This week on Security Now!

- Follow up on law enforcement iOS device unlocking under warrant
- Mozilla's life after Google
- Microsoft responds to Dell's epic mistake
- Arris cable modems in the doghouse
- Blackberry say "no" to a large government
- 67 companies being sued for using HTTPS / TLS Elliptic Curve Crypto on their web sites
- Another welcome nail in the Adobe Flash coffin.
- A bit of miscellany
- 10 questions and answers from our listeners.

Mozilla: *"We don't need Google's money anymore"*



Security News:

Last week's thoughts about warranted iPhone unlocking

- Certainly not very popular with... well... anyone.
- Our smart listeners suggested endless ways that the system could fail.

Mozilla says: "We don't need Google's money anymore."

- http://www.cnet.com/news/firefox-maker-mozilla-we-dont-need-googles-money-anymore/
- In 2014, Mozilla's relationship with Google accounted for most of their $330 million in revenue.
- That was the final year of their paid relationship.
- Mozilla has moved to regional search engine relationships:
  - Yahoo in the United States
  - Baidu in China
  - Yandex in Russia.
- Mozilla gets no revenue at all from Google, even though Google is still the default search engine for Firefox users in Europe.
- Mozilla is holding its own financially and expects to keep doing so without Google's money. Its $330 million in 2014 revenue is up from its $314 million in 2013.
- Chief Financial Officer Jim Cook indicated that the current year's figure will be even better, given Mozilla's new, "very strong" search deals.
- Cook said: "We really look forward to displaying our results next year. 2015 will show our continued track record of really strong financial results."

Microsoft updates their Certificate Trust List (CTL) to block Dell's dangerous certs

- https://technet.microsoft.com/library/security/3119884.aspx
- "Inadvertently Disclosed Digital Certificates Could Allow Spoofing"
- Nov 30th, 2015 - 3119884
- Microsoft is aware of unconstrained digital certificates from Dell Inc. for which the private keys were inadvertently disclosed. One of these unconstrained certificates could be used to issue other certificates, impersonate other domains, or sign code. In addition, these certificates could be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks against Dell customers. This issue affects all supported releases of Microsoft Windows. Microsoft is not currently aware of attacks related to this issue.

  To help protect customers from potentially fraudulent use of these unconstrained digital certificates, the certificates have been deemed no longer valid by Dell Inc. and Microsoft is updating the Certificate Trust list (CTL) for all supported releases of Microsoft Windows to remove the trust of these certificates.

  An automatic updater of certificate trust lists is included in supported editions of Windows 8, Windows 8.1, Windows RT, Windows RT 8.1, Windows Server 2012, Windows Server 2012 R2, Windows 10, and Windows 10 Version 1511, and for devices running Windows

Phone 8 , Windows Phone 8.1, and Windows 10 Mobile. For these operating systems and devices, customers do not need to take any action as these systems and devices will be automatically protected.

For systems running Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 that are using the automatic updater of certificate trust lists (see Microsoft Knowledge Base Article 2677070 for details), customers do not need to take any action as these systems will be automatically protected.

- An automatic updater of revoked certificates is available for Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2
    - https://support.microsoft.com/en-us/kb/2677070
    - http://bit.ly/sn-536

Arris Cable Modems have Double Back Doors

- http://www.scmagazine.com/600000-cable-routers-found-to-have-a-backdoor-within-a-backdoor/article/456352/
- http://www.dslreports.com/shownews/600000-Arris-Cable-Modems-Have-Double-Back-Doors-135709
- http://arstechnica.com/science/2015/11/researchers-poke-hole-in-custom-crypto-protecting-amazon-web-services/
- Bernardo Rodrigues is a vulnerability tester with Brazil's Globo TV network.
- The firmware of many Arris modems ship with an undocumented "libarris_password.so" library, which acts as a backdoor by allowing privileged account logins with a different custom password for each day of the year.
- This ARRIS password of the day is a remote backdoor known since 2009 and still intact.
    - http://www.borfast.com/projects/arris-password-of-the-day-generator
- The default seed is MPSJKMDHAI and many ISPs won't bother changing it at all
    - (DSLReports noted that Comcast told them they don't use the default, so Comcast users won't be at risk until the non-default Comcast seed is determined.)
- At least the Arris models: TG862A, TG860A, and DG860A
- A Shodan search engine revealed 600,000 devices.
- Then the lower five digits of the modem's serial number.
- “You get a full busybox shell when you log on the Telnet/SSH session using these passwords,” Rodrigues said, while adding that Arris requested him not to reveal details about the modem’s password generation algorithm.
- Arris: We are aware of the recently reported password vulnerability. The risk related to this vulnerability is low, and we are unaware of any exploit related to it. However, we take these issues very seriously and review them with the highest priority. Our team has been working around the clock on modem updates that address this reported vulnerability."

Blackberry says "No" to Pakistan

- BlackBerry to leave Pakistan rather than open servers to authorities
- http://www.cp24.com/lifestyle/technology/blackberry-to-leave-pakistan-rather-than-open-servers-to-authorities-1.2680375
- WATERLOO, Ontario: BlackBerry is standing firm on its promise to close its operations in Pakistan rather than accept that country's demands for "unfettered" access to its BES servers, even after a one-month delay in the government's deadline.

  Blackberry blogged that it will continue to operate until December 30th as a result of a one-month extension to a compliance order issued by the Pakistan Telecommunications Authority in July.

  BlackBerry had said previously that it would pull out of Pakistan rather than comply with a demand for full access to content on its BlackBerry Enterprise Service by Nov. 30.

  The company says the Pakistani government wants the ability to monitor all traffic in the country, including every BES email and BES BBM. BES communications are routed through the company's servers in Canada.

  BlackBerry says it's willing to work with Pakistani authorities to protect public safety, but that the privacy of its customers is paramount and something on which it won't compromise.

  BlackBerry's chief of operations operations, Marty Beard, said that the company recognizes the need to co-operate with lawful government investigations of criminal activity, but it has never permitted wholesale access to BlackBerry servers.

  Saudi Arabia and the UAE threatened to ban Blackberry in 2010 when Blackberry refused to hand over control of customer data.

"Eastern District of Texas"-based "CryptoPeak" has sued 66 companies for their use of Elliptic-Curve Crypto in TLS

- US6202150: https://patents.google.com/patent/US6202150B1/en
  - Auto-escrowable and auto-certifiable cryptosystems
  - Original Assignees: Adam & Marcel Yung
  - Filed: May 28th, 1997
  - Granted: March 13th, 2001
- 1st batch of filings were in July, November 9th, 20th, 25th
- Sony, Macy's, AT&T, Pinterest, Netflix, Yahoo, Hyatt Hotels, Priceline, Best Western, Experia, GoPro,, Progressive Insurance
- https://search.rpxcorp.com/advanced_search/search_litigations#searchq=lit_party_ent_id_lms%3A958432&grouped=true&search_type=litigations&utf8=%E2%9C%93

- Complaint: Upon information and belief, Defendant has infringed and continues to directly infringe one or more claims of the ‘150 Patent, including at least claim 1, by actions comprising making, having made, and/or using one or more websites that operate in compliance with the standards of Elliptic Curve Cryptography (“ECC”) Cipher Suites for the Transport Layer Security (“TLS”) protocol (the “Accused Instrumentalities”). A representative example of a website of Defendant that operates in compliance with this standard is secure.livevol.com.
- Netflix files a motion to dismiss:
  - https://regmedia.co.uk/2015/11/30/cryptopeaknetflixmotion.pdf

Abode renames "Adobe Flash Professional" to "Adobe Animate CC"

- http://techcrunch.com/2015/12/01/adobe-puts-another-nail-in-flashs-coffin/
- Techcrunch: Adobe Puts Another Nail In Flash's Coffin
- Adobe:

  "For nearly two decades, Flash Professional has been the standard for producing rich animations on the web. Because of the emergence of HTML5 and demand for animations that leverage web standards, we completely rewrote the tool over the past few years to incorporate native HTML5 Canvas and WebGL support. To more accurately represent its position as the premier animation tool for the web and beyond, Flash Professional will be renamed **Adobe Animate CC**, starting with the next release in early 2016.

  Today, over a third of all content created in Flash Professional today uses HTML5, reaching over one billion devices worldwide. It has also been recognized as an HTML5 ad solution that complies with the latest Interactive Advertising Bureau (IAB) standards, and is widely used in the cartoon industry by powerhouse studios like Nickelodeon and Titmouse Inc.

  Animate CC will continue supporting Flash (SWF) and AIR formats as first-class citizens. In addition, it can output animations to virtually any format (including SVG), through its extensible architecture.

- The tool can be used to author and produce Flash, HTML5 or WebGL.
- HTML5 and WebGL work ubiquitously on mobile. iOS is famously flash hostile.
- Who here thinks Flash has a bright future?

Miscellany

Bill Griffith (@bigpawzzz)

- @SGgrc "Why Zebras Don't Get Ulcers" is on sale on Audible! $4.95.
  I got it. Excellent call. Thanks once again for your recommendations

- Why Zebras Don't Get Ulcers, Now in its 3rd edition
  - https://en.wikipedia.org/wiki/Robert_Sapolsky
    Wikipedia: Robert Morris Sapolsky (born 1957) is an American neuroendocrinologist, professor of biology, neuroscience, and neurosurgery at Stanford University, researcher and author. He is currently a professor of biological sciences, and professor of neurology and neurological sciences and, by courtesy, neurosurgery, at Stanford University.

iPad Pro + Pencil

- It's still too large

SpinRite

Cornel DeLorean
Location: San Mateo, CA
Subject: SpinRite saves the day again
Date: 30 Nov 2015 08:09:42
:
Hi Steve,

I'm a long time listener and owner of SpinRite, I purchased my copy back in 2009 to support you and the podcast but I also figured at some point I would get a chance to rescue a disk and after all these years that time came.

I was helping a friend with his laptop, it was running slow and hanging so after poking around for a bit and removing some unneeded and expired software from McAfee, I rebooted and it refused to boot up. I tried every trick I learned from doing many years of desktop support but nothing worked so I thought let's see if SpinRite can save the day.

I started the scan on Level 2 and it happily got to 48% after about 40 minutes but then it slowed way down. It ran overnight and by morning it was at 51%, when I got home from work at the end of the day, it had crawled up to 53%. I let it run overnight again and it was finally finished when I checked it in the morning.

I rebooted it with fingers crossed and sure enough, it booted right up. I backed up all of his data and advised him it was time for a new laptop but it ran fine for a number of months until he did get a replacement.

Thanks for such a great product and podcast!