Security Now! #468 - 08-12-14

Q&A #194

Link Tracking Warning!
This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

This week on Security Now!

- Patch Tuesday
- BadUSB follow-up
- The Crypto-Unlocker Victim Database
- Russian Hacker's Billion-Password Repository
- Google's Security-biased Website Ranking
- Today's LastPass Outage
- Are your potato chips spying on you?

Today is the final episode of our 9th year!

NEXT Tuesday will be August 19th, 2014, and
August 19th, 2005, was our 1st SN podcast.

Security News:

Patch Tuesday / Nine Patch Bulletins

- 1st (most severe): All versions of IE.
- 2nd most: Windows 8 & 8.1, Media Center TV pack for Vista.
  - Graphics processing pipeline vulnerability.
- 3rd OneNote in Office 2007
- ... and additional elevation of service vulnerabilities.

BadUSB and DFU - Device Firmware Upgrade

- http://www.usb.org/developers/devclass_docs/usbdfu10.pdf

CryptoLocker Victim Database Found

- Repository of private keys obtained...
- https://www.decryptcryptolocker.com/
- Provide an eMail address (for key receipt) and a sample encrypted file.
- <Fireeye quote>: To help solve the problem of victims' files still being encrypted, we leveraged our close partnership with Fox-IT. We developed a decryption assistance website and corresponding tool designed to help those afflicted with the original CryptoLocker malware. Through various partnerships and reverse engineering engagements, Fox-IT and FireEye have ascertained many of the private keys associated with CryptoLocker. Having these private keys allows for decryption of files that are encrypted by CryptoLocker.

- Great writeup/backgrounder on Cryptolocker's history:
- http://blog.fox-it.com/2014/08/06/cryptolocker-ransomware-intelligence-report/
- http://grahamcluley.com/2014/08/fix-cryptolocker-files-free/
- http://www.bbc.com/news/technology-28661463

Russian Hackers Amass Over a Billion Internet Passwords

- http://mobile.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html
- http://www.cnet.com/news/to-stop-security-breaches-kill-the-username-and-password/
- A Russian crime ring has amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses.
- Milwaukee-based "Hold Security"
- Alex Holden, founder and CIO told the NYT: “Hackers did not just target U.S. companies, they targeted any website they could get, ranging from Fortune 500 companies to very small websites... and most of these sites are still vulnerable.”
- The hacking ring is based in a small city in south central Russia, the region flanked by Kazakhstan and Mongolia. The group includes fewer than a dozen men in their 20s who know one another personally — not just virtually.
- Victim PCs are botnet infected and test every website visited for SQL-injection vulnerabilities. When the site responds to an SQL injection it is flagged and reported for later full database dumping.
- By July, the criminals had collected 4.5 billion records — each a user name and password — though many overlapped. After sorting through the data, Hold Security found that 1.2 billion of those records were unique. Because people tend to use multiple emails, they filtered further and found that the criminals’ database included about 542 million unique email addresses.

Google to Prioritize Websites

- http://www.bbc.com/news/technology-28687513
- It might a quality metric?? albeit a weak one.
- Google's blog posting: "For now it's only a very lightweight signal - affecting fewer than 1% of global queries, and carrying less weight than other signals such as high-quality content - while we give webmasters time to switch to HTTPS. But over time, we may decide to strengthen it, because we'd like to encourage all website owners to switch from HTTP to HTTPS to keep everyone safe on the web."

Apple iPhone Privacy Changes Lead to Layoffs at Retail Tracking Startup Nomi

- http://recode.net/2014/08/08/apple-iphone-privacy-changes-lead-to-layoffs-at-retail-tracking-startup-nomi/
- WiFi roaming MAC address randomization produces layoffs...
- Recode: Nomi, a startup that has raised $13 million in venture capital, has laid off at least 20 of its 60 or so employees, in part because of these forthcoming changes, according to sources.
- (Deeper Dig): So... They're switching from WiFi tracking to Bluetooth Beacon tracking, and Bluetooth requires fewer people to setup.

Your bag of potato chips might be spying on you!

- http://newsoffice.mit.edu/2014/algorithm-recovers-speech-from-vibrations-0804
- Extracting audio from visual information / Algorithm recovers speech from the vibrations of a potato-chip bag filmed through soundproof glass.
- Researchers at MIT, Microsoft, and Adobe have developed an algorithm that can reconstruct an audio signal by analyzing minute vibrations of objects depicted in video.
- In one set of experiments, they were able to recover intelligible speech from the vibrations of a potato-chip bag photographed from 15 feet away through soundproof glass.
- In other experiments, they extracted usable audio from videos of aluminum foil, the surface of a glass of water, and even the leaves of a potted plant.
- The researchers will present their findings in a paper at this year's Siggraph, the premier computer graphics conference.
- The good news: Harry Nyquist to the rescue.
    - Western wagon wheels spinning backwards
    - Researchers used high-speed 2,000 to 6,000 fps video!
    - 60 fps might identity gender, number of speakers... MAYBE an identity.

LastPass Outage

- http://blog.lastpass.com/2014/08/update-on-lastpass-connectivity-errors.html

Record all interactions with Comcast

- Tech News Today / Another Comcast fiasco.
- Reversed themselves only after he played them his recording.
- "All party consent" -- NOTIFY agent that you're recording.

SQRL:

- 1st week's testing went very smoothly.
- Now working on encoding an identity into QR code for

SpinRite:

Joe White in Honea Path, SC (honey-ah-path)
Subject: (spinrite) A resurrection at a funeral home

Hey Steve and Leo. Thanks for the show. I've been through the archives and digested them *all*.

I'm a funeral director at a small family funeral home, and being in a family business means wearing many hats. IT is one of my hats. One of our main workstations went down a couple of weeks ago, refusing to recognize it's hard drive any longer. I brought in my copy of SpinRite, let it do it's thing at level 2, and presto, it began working again. Our massive list of outlook contacts has been saved from destruction! I've imaged the drive just to be safe, but it appears that the level 2 scan has restored it to useful service.

Our thanks to you, Steve, for turning our mourning into gladness.
I think a site-license purchase is in order :)