Security Now! #486 - 12-16-14

Q&A #203

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!

- More upcoming Chrome UX changes in 2015,
- A previously secret devastating cyber attack,
- The ethics of disclosing illegally obtained content,
- The legality of disclosing... and Sony's new questionable press strategy,
- Verizon's ridiculous cypher-phone app,
- Miscellaneous goodies & great conversation topics from our listeners.

Security News:

Google proposing to begin marking "HTTP" as "Non-Secure" during 2015.

- https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure
- <quote>

  We, the Chrome Security Team, propose that user agents (UAs) gradually change their UX to display non-secure origins as affirmatively non-secure. We intend to devise and begin deploying a transition plan for Chrome in 2015. The goal of this proposal is to more clearly display to users that HTTP provides no data security.

  We'd like to hear everyone's thoughts on this proposal, and to discuss with the web community about how different transition plans might serve users.

  We all need data communication on the web to be secure (private, authenticated, untampered). When there is no data security, the UA should explicitly display that, so users can make informed decisions about how to interact with an origin.

Sheldon Adelson & Sands struck HARD by cyberattack

- http://www.businessweek.com/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas
- February 10th -- The Sheldon Adelson Sands properties Venetian and Palazzo were struck by a devastating cyberattack... which had been kept secret for the past 10 months.
- Servers crashing, drives being wiped... a direct attack on a corporate infrastructure intended to severely damage the target.
- <quote> This was no Ocean's Eleven. The hackers were not trying to empty a vault of

cash, nor were they after customer credit card data, as in recent attacks on Target (TGT), Neiman Marcus, and Home Depot (HD). This was personal. The perpetrators wanted to punish the company, or, more precisely, its chief executive officer and majority owner, the billionaire Sheldon Adelson. Although confirming their conjectures would take some time, executives suspected almost immediately the assault was coming from Iran.

This was new. Other countries have spied on American companies, and they have stolen from them, but this is likely the first time—occurring months before the late November attack on Sony Pictures Entertainment (SNE)—that a foreign player simply sought to destroy American corporate infrastructure on such a scale. Both hacks may represent the beginning of a geopolitically confusing, and potentially devastating, phase of digital conflict. Experts worry that America's rivals may have found the sweet spot of cyberwar—strikes that are serious enough to wound American companies but below the threshold that would trigger a forceful government response. More remarkable still, Sands has managed to keep the full extent of the hack secret for 10 months.

- Adelson is a staunch and vocal supporter of Israel. And several months before the attack Adelson had spoken out using extremely threatening and provocative language against Israel's arch foe, Iran.

- Read the entire piece: http://bit.ly/sands-attack
- It contains LOTS of interesting technical details which, so far, the Sony story is lacking:

On the Ethics of Disclosure

- http://www.bloombergview.com/articles/2014-12-15/keep-publishing-the-sony-emails
- Last week on SN and on Sunday's TWiT.
- The definition of: "In the public interest"
    - The Snowden leaks: Yes, clearly.
    - The NSA and law enforcement would disagree... and that's the point.
    - But the DIRECT UPSHOT of Snowden was a year of RADICAL change in the industry's security posture:
        - Apple has released phones they cannot decrypt and Google has announced that's on the way.
        - Many 3rd-party communications apps are explicitly designed to offer and are featuring well-designed true end-to-end encryption.
        - True "TNO" security has quickly evolved from something we care about on this podcast... to something everyone cares about.

- Is the NSA happy? NO! Is Sony happy? NO! But human nature is such that that's the way it has to be: Someone has to painfully LOSE in order for everyone else to really get the message.

- Therefore... I would argue that publishing salacious details IS in the long term interest of the public. Not because I have any interest in executive underwear... but because otherwise it's too easy to dismiss the danger of lax security... and true security is annoying, difficult, non-default, and expensive.

Shooting the Messenger -- Sony threatens the Press:

- http://krebsonsecurity.com/2014/12/in-damage-control-sony-targets-reporters/
- Brian Krebs:

  Over the weekend I received a nice holiday letter from lawyers representing Sony Pictures Entertainment, demanding that I cease publishing detailed stories about the company's recent hacking and delete any company data collected in the process of reporting on the breach. While I have not been the most prolific writer about this incident to date, rest assured such threats will not deter this reporter from covering important news and facts related to the breach.

  "SPE does not consent to your possession, review, copying, dissemination, publication, uploading, downloading, or making any use of the Stolen information, and to request your cooperation in destroying the Stolen Information," wrote SPE's lawyers, who hail from the law firm of Boies, Schiller & Flexner.
- http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/12/15/can-sony-sue-media-outlets-who-publish-the-stolen-sony-documents/

Verizon's Voice Cypher

- … Introduced last Thursday with the encryption company Cellcrypt, offers business and government customers end-to-end encryption for voice calls on iOS, Android, or BlackBerry devices equipped with a special app. The encryption software provides secure communications for people speaking on devices with the app, regardless of their wireless carrier, and it can also connect to an organization's secure phone system.

- Cellcrypt and Verizon both say that law enforcement agencies will be able to access communications that take place over Voice Cypher, so long as they're able to prove that there's a legitimate law enforcement reason for doing so.

- Seth Polansky, Cellcrypt's vice president for North America, disputes the idea that building technology to allow wiretapping is a security risk. "It's only creating a weakness when it's a legitimate government agency request. Just because a government access option exists, doesn't mean other companies can access it."

- http://www.verizonwireless.com/wcms/business/apps/voice-cypher.html
- http://www.cellcrypt.com/

- Their slogan: "Security when it matters most"
  <quote> Verizon Voice Cypher by Cellcrypt delivers powerful, end-to-end mobile security solutions. Trust the industry's most secure voice communication for your phones and mobile devices.

Miscellany:

"Ascension" on SyFy

- Mon/Tues/Wed

Isaac Johns in Louisiana notes about Abe...

- Abe's Oddworld has been out for PC for many years…
  The website gog.com has all three a few dollars each.

- http://www.gog.com/game/oddworld_abes_oddysee
- http://www.gog.com/game/oddworld_abes_exoddus
- http://www.gog.com/game/oddworld_strangers_wrath

- And they also sell the collection at a discount; [whole set for $10].

- **Gog sells only the game itself ~not any software DRM that it may have
- originally shipped with.

- Isaac
- [Spinrite customer for many years; Security Now listener since its beginning.]

SpinRite:

Date: Fri, 12 Dec 2014 06:25:36 -0800
To: Security Now Feedback
Subject: SpinRite saved a server RAID array

Steve,

Every weekday morning I do a visual inspection of our servers for any issues (scanning the server status screens and hard drive LEDs). I'm also responsible for backups.

One morning as I was checking the previous evenings backups on one of our NAS servers, I noticed a major read/write error in the backup log causing the backup job to fail completely.

Checking if the backup volume was mounted correctly, I immediately noticed that the volume had disappeared. I then began scouring the system logs and sure enough, we had a drive failure in our RAID 5 array. Come to find out we had another drive failure at a prior time which makes two drive failures at this point causing the entire array to be lost. These two failures slipped by me since the visual inspection on this one custom-built server fails to indicate a problem for any of the drives. It only shows a green LED for power.

Figuring out the problem took only minutes, and looking at what the logs were telling me, my mind immediately went to a previous episode of Security Now. In that episode, you were

discussing how a SpinRite customer was able to save his/her RAID array by removing the drive and booting it as a standalone drive connected via a separate interface. I thought...I can do this. :)

Removed the first failed drive, connected to a laptop via a SATA to USB interface, and booted with SpinRite. I immediately heard some truly awful sounds coming from the drive. Well that sounds bad and sure enough, I could not get SpinRite or the laptop to recognize that one.

Trying the second bad drive, it booted and SpinRite recognized it. Running Level 2, I noticed that at times the drive would seem to have a hard time reading a sector. After a few seconds, it would work through it and on to the next sector.

I ran SpinRite until 50% completion and decided to give it a try back in the server. Sure enough, the drive came back up and the RAID controller gave the okay and the RAID volume is back but in degraded mode since the complete loss of the other drive. I was able to get all of this done within one workday and had backups running again that evening.

I have two new drives on the way and will be replacing them and rebuilding the array as time permits.

Thank you for a great product!