Security Now! #442 - 02-11-14

Q&A #183

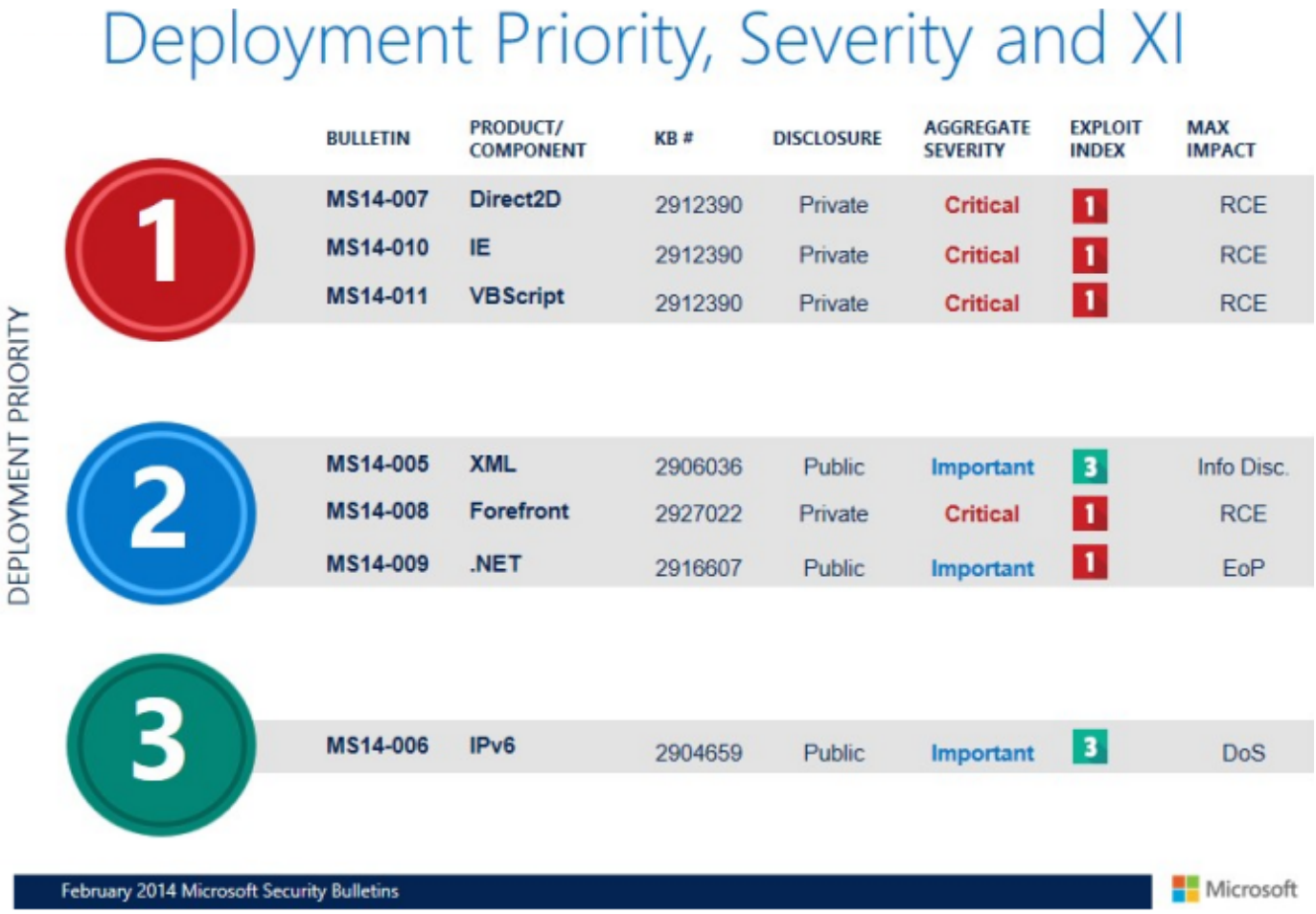
Link Tracking Warning!
This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's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

This Week on Security Now!

- The "Post Password Principles & Policies Podcast"
- Patch Tuesday
- EFF's "Day We Fight Back"
- Today is global "Safer Internet Day"
- Some new details, but still plenty of questions, about the Target POS breach
- Comcast has been upsetting people by turning their homes into PUBLIC WiFi hotspots,
- A SQRL updated... and 10 "largely password related" questions!

The Week's Top News:

Microsoft's Patch Tuesday:



Today -- February 11th, 2014, is officially "Safer Internet Day"

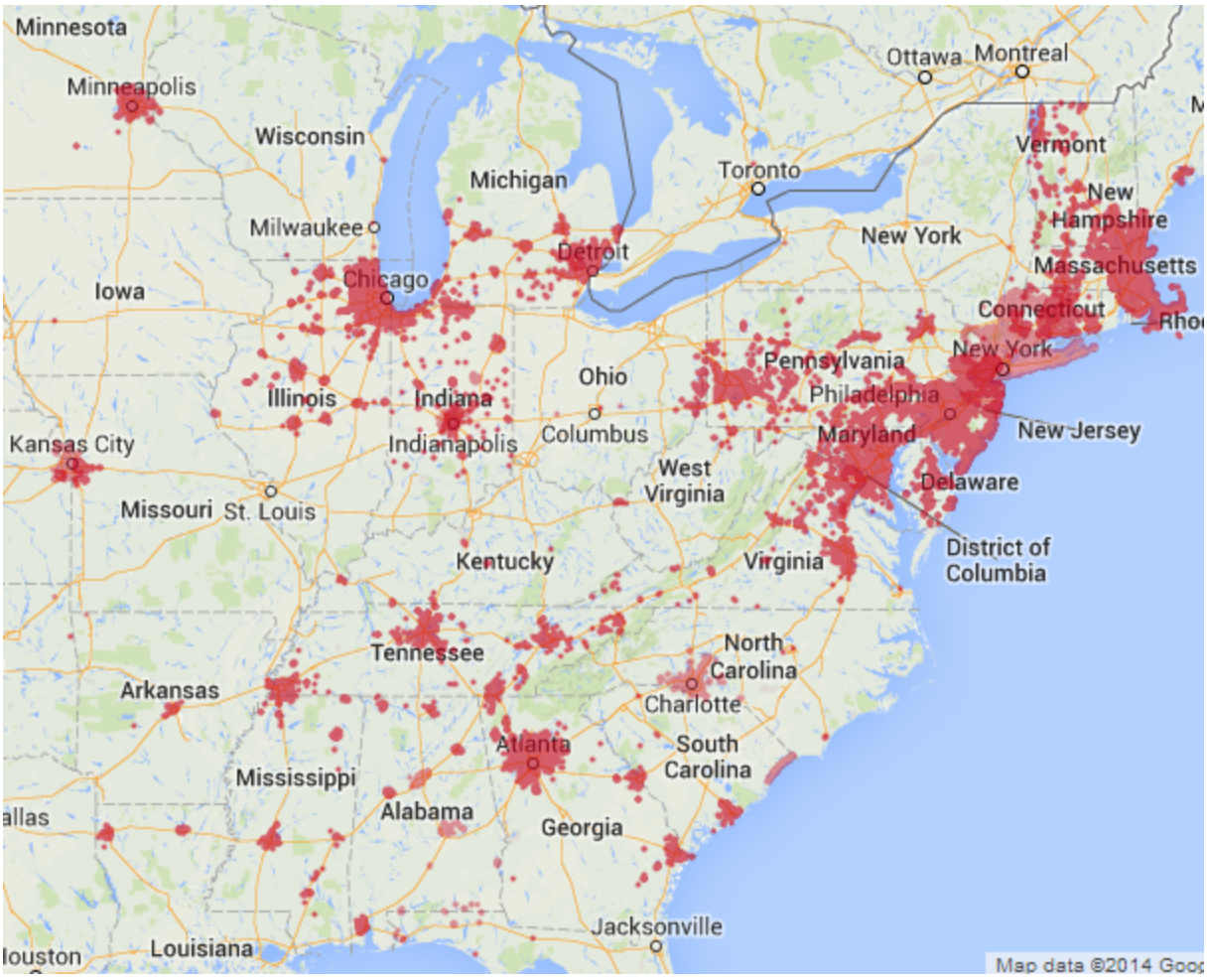
- http://www.saferinternet.org/web/guest/home
- Google's main search page: http://www.google.com/safetycenter/

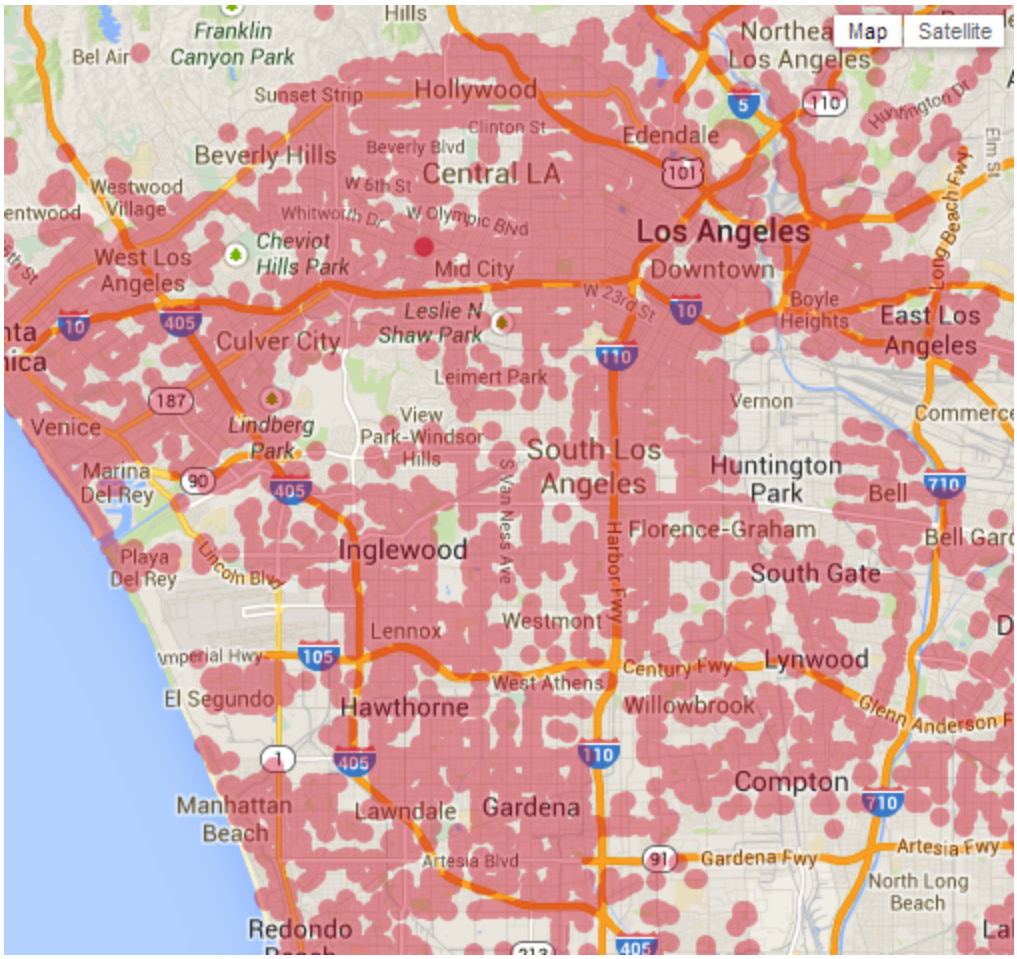
EFF's: "The Day We Fight Back" (Against Mass Surveillance)

- https://www.eff.org/deeplinks/2014/02/today-we-fight-back-against-mass-surveillance
- <quote> Wow. 5,000 people an hour are calling into Congress to demand NSA reform. Join them here, we've made it really easy: https://eff.org/r.pam5

Comcast's weird "WiFi wherever you are" router

- http://bgr.com/2014/02/06/comcast-router-wifi-hotspot-revelation/
- XFINITY WiFi aka "CableWiFi"
- "Over 500,000 Hot Spots. Find One Near You!"
- "With XFINITY WiFi Home Hotspot, you'll have two WiFi networks — one for you and one for your guests. Now you can give visitors WiFi access in your home without sharing your wireless password."





Details of the Target breach

- http://bgr.com/2014/02/06/target-hackers-credentials-theft/
- http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
- ***Brian Krebs*** reports that sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems.
- Fazio's President, Ross Fazio, confirmed that the U.S. Secret Service visited his company's offices in connection with the Target investigation, but said he was not present when the visit occurred.
- Fazio's Vice President, Daniel Mitsch, declined to answer questions about the visit.
- According to the company's homepage, Fazio Mechanical has also performed refrigeration and HVAC work for specific Trader Joe's, Whole Foods and BJ's Wholesale Club locations in Pennsylvania, Maryland, Ohio, Virginia and West Virginia.

- Brian writes: It's not immediately clear why Target would have given an HVAC company external network access, or why that access would not be cordoned off from Target's payment system network. But according to a cybersecurity expert at a large retailer who asked not to be named because he did not have permission to speak on the record, it is common for large retail operations to have a team that routinely monitors energy consumption and temperatures in stores to save on costs (particularly at night) and to

alert store managers if temperatures in the stores fluctuate outside of an acceptable range that could prevent customers from shopping at the store.

- "To support this solution, vendors need to be able to remote into the system in order to do maintenance (updates, patches, etc.) or to troubleshoot glitches and connectivity issues with the software," the source said. "This feeds into the topic of cost savings, with so many solutions in a given organization. And to save on head count, it is sometimes beneficial to allow a vendor to support versus train or hire extra people."

Law firm loses its entire cache of files

- http://news.techworld.com/security/3501017/cryptolocker-scambles-us-law-firms-entire-cache-of-legal-files/

Miscellany:

From the Podcast mailbag:

- Phil in South Florida
  Subject: Your EV Certs
  Date: Mon, 03 Feb 2014

  I was using your SSL fingerprint site and noticed that your EV is set to expire in about 10 days.

  Letting you know so you don't lose any Yabba-Dabba's!

  (Another PERFECT DigiCert experience!)

SQRL:

- Iterating over the design:
  (From a posting I wrote this morning)

- Q: "any estimate on when this might be? I'm currently working on a Bachelor thesis evaluating SQRL and it is quite hard to keep track of all the (ongoing) discussions. Are there any other (major) aspects prone to be changed in the (near) future?

- A: On today's podcast I'm going to talk a bit about the nature of "iterating" over a design. We did this during the development of the Longest Repeated Strings technology, where each iteration substantially improved upon the one preceding... until finally there was actually a breakthrough that was clearly the end of the design.

  The trouble is, this is what happens with unbounded development where a higher value is placed upon eventually arriving at the best possible result, than is placed upon what are effectively arbitrary deadlines. True creativity isn't something that can be demanded my "management", given a timeline budget and placed onto a PERT chart.

As for where we are today? I had no idea when I switched over to thinking about the user interface that it was going to feed backwards and force significant changes to the design of the technology. But that's what makes this entire effort interesting and, I think, worthwhile.

I ***think*** that with yesterday's redesign I'm finally happy with the management of the crypto keying.

SpinRite Field Report:

Who: Matt in Atlanta
Date: Fri, 07 Feb 2014
Subject: SpinRite is the hero; I get the credit

Steve,

I started listening to Security Now 1.5 years ago and have been hooked ever since. During one of the episodes, you described how SpinRite worked and I decided to buy a copy to put it into my IT 'toolbox' on the off chance I ever needed it. Well, tonight was the night! I just took a Graduate Assistant position, doing IT support for a department in my school, and was setting up a KVM switch for a faculty member. Simple job, right? Computers were shut down, cables were hooked up, and power was restored, but....one computer was in an blue screen of death loop and Windows recovery wasn't working. I thought for a second, got a smile on my face, and pulled out my SpinRite CD. Off it went, on Level 2. After it finished, one sector wasn't recovered, so I crossed my fingers and rebooted the computer. The Windows 7 start up sound never sounded so good!

It is finally my chance to say thank you for this awesome product! It will (and should have) come first in line to fix my problems.

Thanks!

Side note, I decided to run SpinRite on the drive a second time and the one unrecovered sector was good! I presume that was just SpinRite doing its thing.