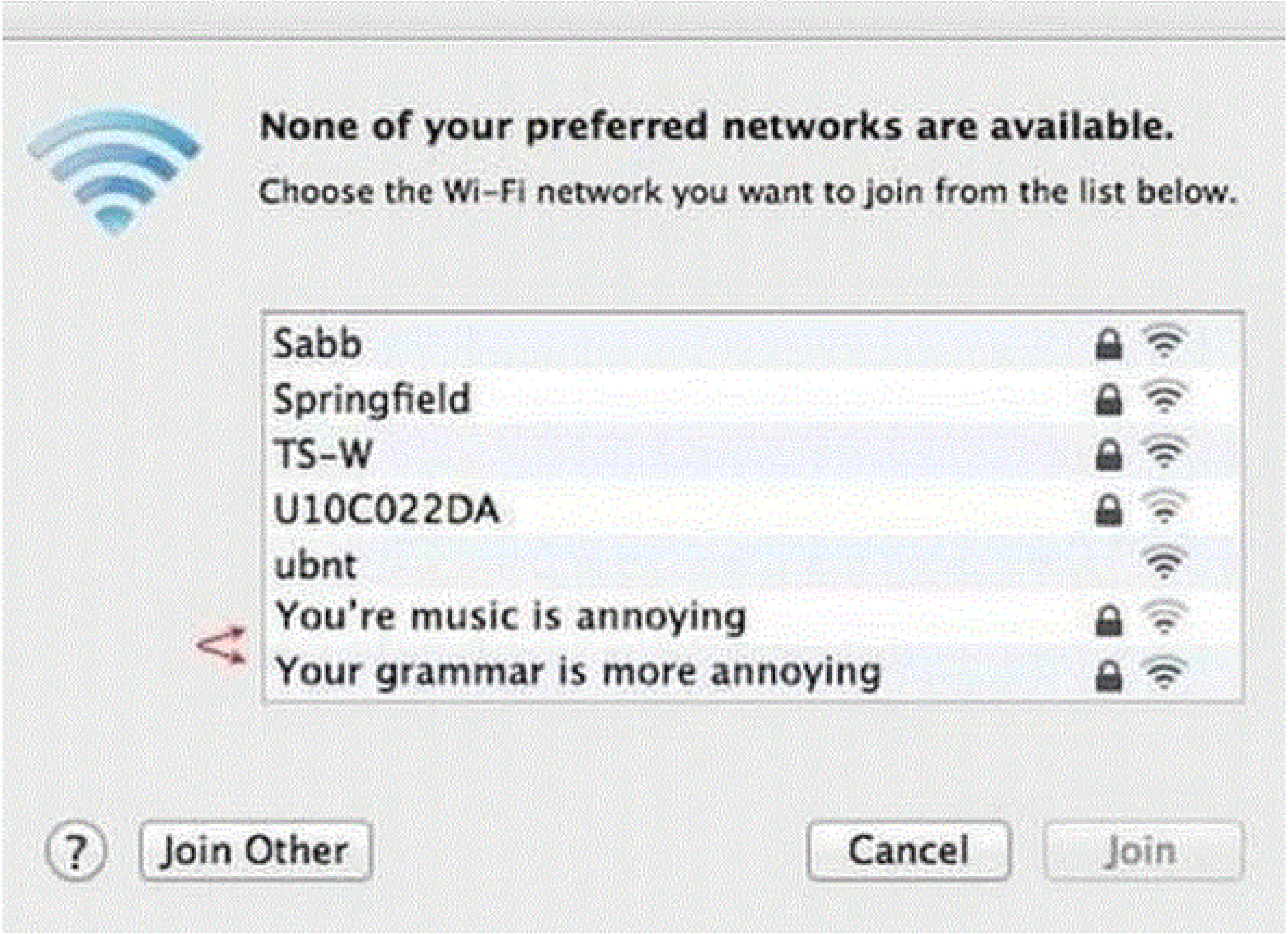
Security Now! #494 - 02-10-15

Q&A #206

This week on Security Now!

- Microsoft’s 55-Vulnerability Patch Tuesday!
- Adobe has been busy patching FLASH,
- The U.S. Government announces a cyber threat integration center,
- The latest news of the Anthem breach,
- Chrome begins the move to HTTP/2,
- Car hacking, TV eavesdropping, GPG gets a new infusion of support, and more!

The Image of the Week, thanks to Simon Zerafa



None of your preferred networks are available.

Choose the Wi-Fi network you want to join from the list below.

Sabb
Springfield
TS-W
U10C022DA
ubnt
You're music is annoying
Your grammar is more annoying

Security News

Microsoft’s 55-Vulnerability Patch Tuesday!

- Microsoft today released nine update bundles
- Eliminates at least 55 distinct security vulnerabilities
- Three of the patches fix bugs in Windows that Microsoft considers “critical”.
- The bulk of the flaws (41) addressed in this update apply to Internet Explorer, the default browser on Windows. This patch should obviously be a priority for any organizations that rely on IE. Other patches fix bugs in the Windows OS itself and in various versions of Microsoft Office. A full breakdown of the patches is available here.
- MS15-009:
  This security update resolves one publicly disclosed and forty privately reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.
- MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220)
  This security update resolves one publicly disclosed and five privately reported vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker convinces a user to open a specially crafted document or visit an untrusted website that contains embedded TrueType fonts.
- TIFF image vulnerability
- Office, Group Policy, VMM, Microsoft Graphics Component

Multiple Adobe FLASH 0-day flaws and patches.

- Being exploited in the wild: Windows, OS X, Linux allowing attackers to execute arbitrary code.
- Within a week of each other.

CTIIC - Cyber Threat Intelligence Integration Center (breaking news today)

- http://www.reuters.com/article/2015/02/10/us-cybersecurity-agency-idUSKBN0LE1EX20150210
- The NSA, DHS, FBI & CIA each have their own cybersecurity groups.
- But there's no central coordination. The intention is for the CTIIC to provide that coordination.
- Similar to the National Counterterrorism Center established after the 9/11 attacks.

Anthem Breach

- http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html?smid=tw-share
- http://time.com/3700203/anthem-identity-theft-hacking/?xid=newsletter-brief
- http://www.scmagazine.com/anthem-breach-what-we-know-so-far/article/396588/
- What we know:
    - 80 Million subscriber identity theft.
        - (Both current and former members.)
    - All lines of Anthem business have been impacted, including Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, Unicare, Healthlink, and DeCare.
    - The information that was compromised includes names, dates of birth, member IDs and Social Security numbers, addresses, phone numbers, email addresses, and employment information, including income data.
    - Anthem said the information involved was not encrypted in its database.
    - Anthem said additional encryption would not have thwarted the attack because an administrator's credentials were compromised and security protocols were bypassed.
    - http://www.anthemfacts.com/
- Anthem detected the attack themselves and responded immediately both internally and publicly.
- Mandiant was brought in to assess...
    - Dave Damato, managing director of Mandiant:
    - Confirmed that "[Attackers] were using several custom backdoors that are not publicly available.
    - They had seen variants of them before, but also not publicly known.
    - Damato: Immediately after Anthem noticed the incident they reset some passwords and performed a series of actions to remove the attacker from the environment. Any passwords that were affected by the breach were reset, [and they began] blocking traffic associated with the attacker and removing any compromised systems.
- First apparent unauthorized access to Anthem's database dates back to December 10th.
- Anthem first became aware of suspicious activity on January 27th.

Google announced yesterday that it will soon be adding HTTP/2 support in Chrome 40.

- Google at it best.
- We've been using HTTP/1.1 since 1999 (16 years).
- Primary benefit of HTTP/2 is improved performance.
- SPDY now supported by all major browsers: Chrome, IE, Firefox, Opera, Safari, Amazon's Silk.
- SPDY support will be phased out sometime next year (2016).

Car Hacking

- 60 minutes Demonstration
- Why should braking be overridable? And steering?
- http://consumerist.com/2015/02/09/report-automakers-fail-to-protect-connected-cars-from-security-privacy-hacks/
- http://arstechnica.com/security/2015/02/senator-car-hacks-that-control-steering-or-steal-driver-data-way-too-easy/
- http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf
- http://bit.ly/carhacking   (12-page report)

Your TV is listening...

- Samsung privacy policy warns: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of voice recognition."
- http://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy
- Parker Higgins (@xor) Director of Copyright Activism for the EFF / tweet:
    - Samsung SmartTV privacy policy, warning users not to discuss personal info in front of their TV.
- SAMSUNG:
    - You can control your SmartTV, and use many of its features, with voice commands.

      If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide you the Voice Recognition feature, some voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service that converts speech to text or to the extent necessary to provide the Voice Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

      If you do not enable Voice Recognition, you will not be able to use interactive voice recognition features, although you may be able to control your TV using certain predefined voice commands. While Samsung will not collect your spoken word, Samsung may still collect associated texts and other usage data so that we can evaluate the performance of the feature and improve it.

GPG maintainer *(WAS)* **going broke...**

- Werner Koch created GPG (Gnu Privacy Guard) in 1997 (18 years ago).
- Since 2001, been receiving about $25K/year in GPG donations.
- Several German government grants, but those ran out.
- Was about to call it quits in 2013 when the Edward Snowden story hit.
- Julia Angwin - Feb 5th, 10:24am
    - http://www.propublica.org/article/the-worlds-email-encryption-software-relies-on

    - -one-guy-who-is-going-broke
    - <quote> The World's Email Encryption Software Relies on One Guy, Who is Going Broke
- The week before the story hit, he received a one-time grant of $60K from the Linux Foundation's Core Infrastructure Initiative.
- By 8:10pm:
    - Since the story was posted to the Net:
    - He reached his funding goal of $137K
    - Facebook and online payment processor Stripe both pledged to donate $50K/year.
- https://news.ycombinator.com/item?id=9003791
- https://www.gnupg.org/donate/index.html
- https://digg.com/2015/the-worlds-email-encryption-software-relies-on-one-guy-who-is-going-broke

Slides show Google's thinking about improving SSL warnings:

- http://bit.ly/sslslides
- https://docs.google.com/presentation/d/1TNFx6eaQVfe83PV80-FZ39QY1dSLGCWW8f2i5-NeJ48/present#slide=id.p
- Adrienne Porter Felt / Chrome security team / felt@chromium.org

Miscellany:

- Speaking of slides:
    - http://bit.ly/sqrlslides (offers a PDF)
- "The Expanse"
    - Book #1 down, book #2 underway...

SpinRite:

- James Bliss @JamesBliss
    - Again, thnx to @SGgrc, it appears to others that I have a superpower.
      I do (all thnx to him) & it's called SpinRite. grc.com/sr/whatitdoes.…
- James Munn @salesmunn
    - @patrickklepek get and run SpinRite 6 on it from the great @SGgrc!
      It has rescued many a HD for me.