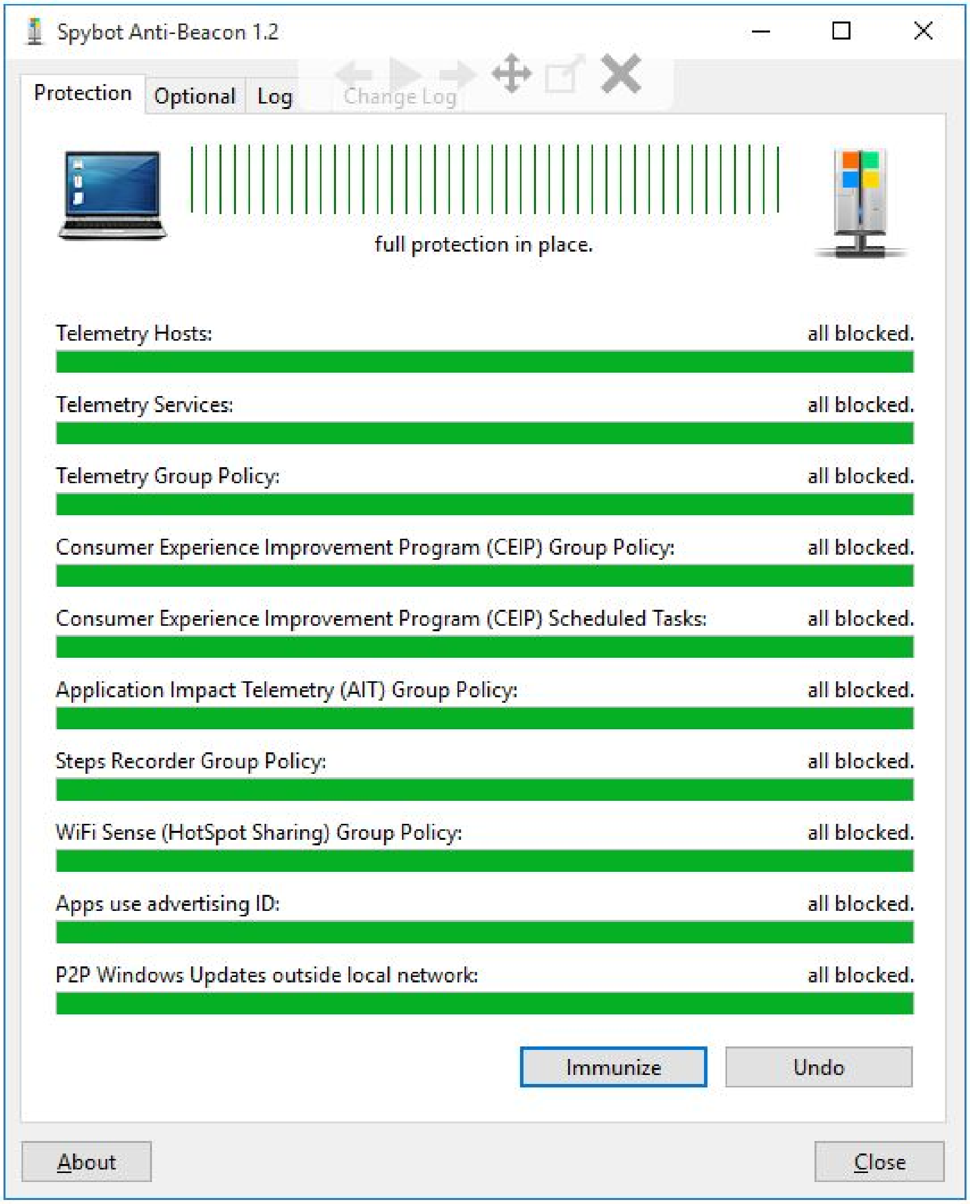
Security Now! #533 - 11-10-15

Q&A #222

This week on Security Now!

- China’s new hiring problem
- Firefox v42 update
- Lots of news about ransomware and Internet extortion
- CAs mis-issuing banned certificates
- Microsoft rethinking their own January 1st 2017 SHA-1 cutoff date
- A ton of fun miscellany with some software tool recommendations

Spybot Anti-Beacon v1.2



full protection in place.

Telemetry Hosts: all blocked.

Telemetry Services: all blocked.

Telemetry Group Policy: all blocked.

Consumer Experience Improvement Program (CEIP) Group Policy: all blocked.

Consumer Experience Improvement Program (CEIP) Scheduled Tasks: all blocked.

Application Impact Telemetry (AIT) Group Policy: all blocked.

Steps Recorder Group Policy: all blocked.

WiFi Sense (HotSpot Sharing) Group Policy: all blocked.

Apps use advertising ID: all blocked.

P2P Windows Updates outside local network: all blocked.

Security News:

Microsoft Patch Tuesday

- Nothing appears Earth shaking
- Windows Journal, Edge and IE have CRITICAL updates, all the rest are “Important”

THE ONION: “China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems”

- http://www.theonion.com/article/china-unable-recruit-hackers-fast-enough-keep-vuln-51719
- BEIJING—Despite devoting countless resources toward rectifying the issue, Chinese government officials announced Monday that the country has struggled to recruit hackers fast enough to keep pace with vulnerabilities in U.S. security systems. “With new weaknesses in U.S. networks popping up every day, we simply don’t have the manpower to effectively exploit every single loophole in their security protocols,” said security minister Liu Xiang, who confirmed that the thousands of Chinese computer experts employed to expose flaws in American data systems are just no match for the United States’ increasingly ineffective digital safeguards. “We can’t keep track of all of the glaring deficiencies in their firewall protections, let alone hire and train enough hackers to attack each one. And now, they’re failing to address them at a rate that shows no sign of slowing down anytime soon. The gaps in the State Department security systems alone take up almost half my workforce.” At press time, Liu confirmed that an inadequate labor pool had forced China to outsource some of its hacker work to Russia.

New Firefox v42

- Private Browsing with Tracking Protection that blocks Web elements that could be used to record cross-site behavior.
- Options / Privacy / Tracking:
    - ○ Request that sites not track you [x]
    - ○ Use Tracking Protection in Private Windows [x]
- https://support.mozilla.org/en-US/kb/tracking-protection-pbm?as=u&utm_source=inproduct
- <quote> "Tracking" refers to the collection of a person’s browsing data across multiple sites. The Tracking Protection feature uses a list provided by Disconnect to identify and block trackers.

  A shield icon will appear in your address bar whenever Firefox is blocking tracking domains. To see which resources are being blocked, you can open the web console and look for messages under the Security tab.
- Indicator added to tabs that play audio with one-click muting.
- WebRTC and Login Manager improvements.

Ransomware & Extortionists retargeting to websites

- http://krebsonsecurity.com/2015/11/ransomware-now-gunning-for-your-web-sites/
- Named:
  - Linux.Encoder.1 by Russian A/V company Dr.Web target Linux web servers.
  - Linux Filecoder, etc.
- Low but increasing detection by VirusTotal
  - https://www.virustotal.com/en/file/fd042b14ae659e420a15c3b7db25649d3b21d92c586fe8594f88c21ae6770956/analysis/
- The malware gains a foothold through known vulnerabilities in site plugins or third-party software.
  - Once on a host machine, the malware encrypts all files in the "home" directories on the system, as well backup directories and most of the system folders typically associated with Web site files, images, pages, code libraries and scripts.

- To cite a specific case:
  - A site was recently infected and encrypted through an unpatched vulnerability in "Magneto", shopping cart software used by many cites to handle eCommerce payments.

  - Checkpoint went public about this vulnerability in April 2015, and notified eBay, Magneto's parent company since 2011.
    - http://blog.checkpoint.com/2015/04/20/analyzing-magento-vulnerability/
    - April 20th, 2015:
    - <quote> Check Point researchers recently discovered a critical RCE (remote code execution) vulnerability in the Magento web e-commerce platform that can lead to the complete compromise of any Magento-based store, including credit card information as well as other financial and personal data, affecting nearly two hundred thousand online shops.

      Check Point privately disclosed the vulnerabilities together with a list of suggested fixes to eBay prior to public disclosure. A patch to address the flaws was released on February 9, 2015. Store owners and administrators are urged to apply the patch immediately if they haven't done so already.

      The vulnerability is comprised of a chain of several vulnerabilities that ultimately allow an unauthenticated attacker to execute PHP code on the web server. The attacker bypasses all security mechanisms and gains control of the store and its complete database, allowing credit card theft or any other administrative access into the system.

      This attack is not limited to any particular plugin or theme. All the vulnerabilities are present in the Magento core, and affects any default installation

  - So Checkpoint notified eBay, Magneto fixed the problem. Checkpoint waited a little over two months for the patches to be applied, then went public with that disclosure.

  - Nevertheless, that site, like so many, was behind on updates for 3rd-party applications... such as their shopping cart software.

- UPDATE: BitDefender discovered that the encryption key was predictable, allowing the files to be decrypted:
    - Linux Ransomware Debut Fails on Predictable Encryption Key
    - http://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/
    - <quote> The AES key is generated locally on the victim's computer. We (BitDefender) looked into the way the key and initialization vector are generated by reverse-engineering the Linux.Encoder.1 sample in our lab. We realized that, rather than generating secure random keys and IVs, the sample would derive these two pieces of information from the libc rand() function, whcih is seeded with the current system timestamp at the moment of encryption. This information can be easily retrieved by looking at the file's timestamp. This is a huge design flaw that allows retrieval of the AES key without having to decrypt it with the RSA public key sold by the Trojan's operator(s).
    - Automated decryption tool now available

- Next Twist... in the wake of the Sony Entertainment scandal, companies are now being told that if they don't pay thousands of dollars to get their data decrypted... the extortionists will post all of their stolen data publicly.

Forbidden certificates have been issued by "many" CAs

- http://arstechnica.com/security/2015/11/https-certificates-with-forbidden-domains-issued-by-quite-a-few-cas/
- COMODO recently performed an internal audit and uncovered 8 certificates that should never have been issued.
- "mailarchive" and "help"
- Comodo also warned that "quite a number" of unnamed competitors have committed similar violations.
- The CA Browser Forum (CAB) operates under a set of "Baseline Requirements" which dictate the behavior for all trusted Certificate Authorities. These rules forbid, among other things, the issuance of certificates for internal names that are not part of the valid Internet domain name or for any of the reserved IP address regions such as 192.168.*.*.

"Power Worm" ransomware cannot sucessfully decrypt files after payment

- http://www.bbc.com/news/technology-34765484
- BBC's Headline: Badly coded ransomware locks away data... forever
- Power Worm infects Microsoft Word and Excel files but the latest poorly written update of it goes after many more types of data files it finds on a victim's machine.

  Malware researcher Nathan Scott discovered the variant and uncovered the mistakes its creator made when updating it. Nathan believes the errors arose when the creator tried to simplify the decryption process. They tried to make it use a single decryption key, but mangled the process of generating it. As a result, there is NO DECRYPTION KEY created for the files it encrypts when it compromises a computer.

  On the Bleeping Computer website, malware researcher Lawrence Abrams wrote: "There is unfortunately nothing that can be done for victims of this infection. If you have been affected by this ransomware, your only option is to restore from a back-up."

Mr Abrams said anyone hit by Power Worm should NOT pay the 2 bitcoin (about £500) ransom it asks for because they will not get any data back.

Microsoft may block SHA1 certificates sooner than expected

- http://blogs.windows.com/msedgedev/2015/11/04/sha-1-deprecation-update/
- "SHA-1 Deprecation Update"
- <quote> In a previous update on TechNet, we announced that Windows will block SHA-1 signed TLS certificates starting on January 1, 2017. In light of recent advances in attacks on the SHA-1 algorithm, we are now considering an accelerated timeline to deprecate SHA-1 signed TLS certificates as early as June 2016.

  Mozilla recently announced a similar intent on the Mozilla Security Blog. We will continue to coordinate with other browser vendors to evaluate the impact of this timeline based on telemetry and current projections for feasibility of SHA-1 collisions.

- Mozilla wrote:
  - https://blog.mozilla.org/security/2015/10/20/continuing-to-phase-out-sha-1-certificates/
  - In our previous blog post about phasing out certificates with SHA-1 based signature algorithms, we said that we planned to take a few actions with regard to SHA-1 certificates:
    - Add a security warning to the Web Console to remind developers that they should not be using a SHA-1 based certificates
    - Show the "Untrusted Connection" error whenever a SHA-1 certificate issued after January 1, 2016, is encountered in Firefox
    - Show the "Untrusted Connection" error whenever a SHA-1 certificate is encountered in Firefox after January 1, 2017

  - In Firefox 43 we plan to show an overridable "Untrusted Connection" error whenever Firefox encounters a SHA-1 based certificate that has ValidFrom after Jan 1, 2016. This includes the web server certificate as well as any intermediate certificates that it chains up to. Root certificates are trusted by virtue of their inclusion in Firefox, so it does not matter how they are signed. However, it does matter what hash algorithm is used in the intermediate signatures, so the rules about phasing out SHA-1 certificates applies to both the web server certificate and the intermediate certificates that sign it.

    We are re-evaluating when we should start rejecting all SHA-1 SSL certificates (regardless of when they were issued). As we said before, the current plan is to make this change on January 1, 2017. However, in light of recent attacks on SHA-1, we are also considering the feasibility of having a cut-off date as early as July 1, 2016.

Security Maintenance Tip of the Week:

- Log into your Twitter Account on the web and scan the Apps you have given access.

Quote of the Week:

- chriskeller (@chriskeller)
  @SGgrc... My password is the last 15 digits of Pi. :-)

Miscellany:

Sunday's TWiT Podcast

- WOW! World Class Conference Level Discourse.
- What you would pay thousands of dollars and travel thousands of miles to hear.
- Truly wonderful. VERY different from Security Now!... and wonderfully so.

Fabulous Network Bandwidth Usage Monitor:

- SoftPerfect "NetWorx" -- Free
    - Stunning feature set.
        - Instantaneous bandwidth usage.
        - Long term usage aggregation
        - Per-App usage
        - customization.

Spybot Anti-Beacon for Win7-10

- https://forums.spybot.info/downloads.php?cat=1
- Installer / Portable / Standalone versions
- Description:
  Spybot Anti-Beacon for Windows 10 is a small utility designed to block and stop the various tracking (aka telemetry) issues that come with Windows 10. Seeing the bunch of incomplete or broken scripts to disable tracking in Windows 10, and the tools that install adware or worse in exchange for their function, we wrapped disabling tracking up in a small tool that’s free and clean. With the upcoming news about telemetry in Windows 7 and 8.1, Spybot Anti-Beacon has added support for those as well.

"Alarmed" - iTunes

- Pop-up reminder alerts with robust repeat scheduling, flexible snooze and full customization.
- Pop-up timers with custom messages, countdown / count up, timer queues and more.
- Support for both timed and location reminders.
- Use Siri to create reminders and import from the Reminders app into Alarmed.
- iCloud syncing & backup. (Extras Package)
- Notes-as-checklist instantly transforms notes into actionable checklists.
- Categories to help you organize your reminders and timers.
- Over 140 high-quality custom sounds included.
- Are you alarmed?

"Spectre"

- Fabulous - Everything you want from a Daniel Craig Bond movie!

Thurrott on the iPad Pro:

- "Thin. Light. Pointless."
- https://www.thurrott.com/mobile/ios/7740/thinking-about-the-ipad-pro

SpinRite:

"Change your drive's oil periodically with SpinRite"
Barry Brown: Arizona in the winter, Washington in the summer

Subject: SpinRite Oil Change
Steve, I've been using SpinRite monthly, for many years, on my 8 year old HP9500 laptop. I have the original drive that came with the laptop still in use as the D: drive where I store data. About 4 years ago I upgrade the C: drive to as SSD. And needless to say, I've never had any trouble with either of them.

If you want your internal combustion engine to last, you change the oil. If you want your hard drives and SSDs to last, you run SpinRite.

This laptop has not led an easy life. I use it as my portable desktop, it has been all over the world and even fell out of the overhead bins a few times. SpinRite brought it back, time and again.

Barry