Security Now! #458 - 06-03-14

TrueCrypt: WTF?

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 troubling misuse of the US Computer Fraud & Abuse Act,
- Chrome meaningfully tightens security,
- Brian Williams & Edward Snowden,
- ZeuS Botnet & Cryptolocker are (apparently) paused for two weeks,
- Apple's WWDC & iOS8,
- Halt & Catch File,
- My final comments on the world's best and most economical shave...
- And... the VERY bizarre past week with TrueCrypt: WTF?

Security News:

US cybercrime laws being used to target security researchers

- US Computer Fraud and Abuse Act (CFAA).
- http://www.theguardian.com/technology/2014/may/29/us-cybercrime-laws-security-researchers
    - Security researchers say they have been threatened with indictment for their work investigating internet vulnerabilities.
- "If you go public with this we'll pursue you under the CFAA."

Chrome tightens extension security:

- Santiago Barcia @SewardJack
- Chrome extension ecosystem looking more and more like Apple's chrome.blogspot.com/2014/05/protec… @SGgrc I guess it's good for security?!
- Protecting Chrome users from malicious extensions
    - http://chrome.blogspot.com/2014/05/protecting-chrome-users-from-malicious.html
    - Extensions can ONLY be installed from the Chrome Web Store.
    - Extensions that were previously installed may be automatically disabled and cannot be re-enabled or re-installed until they're hosted in the Chrome Web Store.
    - Exceptions made for developers who need local installation.

Snowden's Brian Williams NBC interview

CryptoLocker: global police operation disrupts one of most aggressive viruses ever

- Monday, the US DOJ announced that a federal court in Pittsburgh allowed the FBI to:
  - <quote> redirect the automated requests by victim computers for additional instructions away from the criminal operators to substitute servers established pursuant to court order.
- GameOver ZeuS Botnet:
  - Security researchers estimate that between 500,000 and 1 million computers worldwide are infected with Gameover Zeus, and that approximately 25 percent of the infected computers are located in the United States. The total losses worldwide are unknown, but we believe that losses exceed $100 million to U.S. victims alone. Because many of the victims are small- and mid-sized businesses, their accounts typically do not have the same legal protections afforded to consumer accounts, so such losses can be devastating.
- http://www.theguardian.com/technology/2014/jun/02/cryptolocker-virus-nca-malware-protection
  - <quote> "Internet users now have two weeks to protect themselves, warns UK's National Crime Agency after working with Europol and FBI" ***HUH??????***
- Also:
  - http://www.nationalcrimeagency.gov.uk/news/news-listings/386-two-week-opportunity-for-uk-to-reduce-threat-from-powerful-computer-attack

Miscellany:

WWDC & iOS8:

- My personal iOS8 Favorites:
  - Inter-Application Communications
  - Curated, sandboxed, interactions
  - Safari browser extensions?
    - LastPass built-in??
  - Custom Keyboards
    - Fleksy - beta signup now.
    - SwiftKey
  - QuickType (maybe)
  - TouchID for 3rd-party Apps
    - People are worried, but it can be done securely.
  - “Per App” Battery Usage.
  - HomeKit.

HCF - Halt and Catch Fire

- Promising & Fun...

Harry's:

- pdevlin (@cloudyparts) / 12:36pm · 1 Jun 2014
    - @SGgrc Thank you @harrys 4 the best shave in 20yr. Wife & daughter are ecstatic at pain-free kisses. Maybe they'll stop calling me poki-man!

- Santiago Barcia (@SewardJack) / 3:11pm · 1 Jun 2014
    - shaved 1.Harry's 2.Gillette 3. Harry's 4. Gillette ALL NEW blades, Harry's slightly better than Gillette but much cheaper, thanks @SGgrc

- Ronald Collins (@Silfen) / 3:39pm · 1 Jun 2014
    - @SGgrc Great call on @harrys, love my Winston kit. Though I can no longer use my 6-months-same-as-cash-for-blades joke when I shop.

- Jared (@security_spec) / 9:30pm · 1 Jun 2014
    - @SGgrc 3rd day shaving. Best shave every. Love my @harrys razor & cream. No skin irritation. Almost as close as a straight edge razor...

SpinRite:

Jason in Portland, Oregon
Subject: SpinRite isn't obsolete yet
Date: Tue, 20 May 2014 04:42:10 -0000

Steve,

Lately, I've been wondering if SpinRite has been rendered obsolete by SMART and sophisticated drive technology. Could it be that SpinRite's supposed miracles are simply because it forces the drive to take a hard look at itself, and all of the repairs are being handled the drive itself? I wondered if booting from another drive and running `cat /dev/sda > /dev/null` would accomplish the same thing as a Level 2 scan by virtue of reading every sector?

I found the answer last night. I updated GRUB (my boot loader) some time ago and just noticed that my seldom-used Windows drive was no longer on the list. I tried a few tricks to get it to boot, but Windows would always partially load and then the system would reboot.

So, I reached for SpinRite and ran Level 2 on the drive. When it was complete, I tried booting again but the symptoms were unchanged. Next, I got aggressive. I started Level 5, and went to bed.

When I awoke, the scan was about 1/3 complete, but I tried booting the drive anyway. It was a success. Windows loaded right up! I finished the scan for good measure, ran `update-grub2` from my main OS, and I'm back in business.

This experience shows that drives aren't yet smart enough to take care of themselves. Thanks for the great product and your wonderful shows with Leo.
Jason. Portland, Oregon.

TrueCrypt: WTF?

Since last Tuesday's Q&A Podcast

- Three blog posts
- Appearances on TNT with Mike Elgan and Tom Merritt's podcast.
- A new very-high-traffic page at GRC.
- A new TrueCrypt Repository at GRC with off-site confirmation hashes.
- Renegotiating my bandwidth contract with Level3.

Bizarre:

- First line in red: WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues

- Then:
  - This page exists only to help migrate existing data encrypted by TrueCrypt.

    The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windows XP. Windows 8/7/Vista and later offer integrated support for encrypted disks and virtual disk images. Such integrated support is also available on other platforms (click here for more information). You should migrate any data encrypted by TrueCrypt to encrypted disks or virtual disk images supported on your platform.

- Then:
  - Detailed instructions for migrating encryption from TrueCrypt to Bitlocker.

- Then:
  - Download: WARNING: Using TrueCrypt is not secure
  - You should download TrueCrypt only if you are migrating data encrypted by TrueCrypt.
  - TrueCrypt 7.2 sig key
  - If you use TrueCrypt on other platform than Windows, click here.
  -
  - The SITE looked like a quick hack... but the CODE was IMMACUTELY and painstakingly edited.

Naturally, the press exploded with half-baked conspiracy theories:

- Warrant Canary: Served with an NSL (national security letter) and pulled a Lavabit.
- The continuing crypto audit WOULD discover something, so the Devs wanted distance now.
- Occam's Razor.
  - We're no longer going to be maintaining this.
  - That being the case, future problems will not be repaired.
  - We don't want you calling us… so for our sake and your sake, please stop using it.

"David" heard from:
Steven Barnhart (@stevebarnhart) wrote to an eMail address he had used before and received several replies from "David." The following snippets were taken from a twitter conversation which then took place between Steven Barnhart (@stevebarnhart) and Matthew Green (@matthew_d_green):

- TrueCrypt Developer "David": "We were happy with the audit, it didn't spark anything. We worked hard on this for 10 years, nothing lasts forever."
- Steven Barnhart (Paraphrasing): Developer "personally" feels that fork is harmful: "The source is still available as a reference though."
- Steven Barnhart: "I asked and it was clear from the reply that "he" believes forking's harmful because only they are really familiar w/code."
- Steven Barnhart: "Also said no government contact except one time inquiring about a 'support contract.' "
- TrueCrypt Developer "David" said: "Bitlocker is 'good enough' and Windows was original 'goal of the project.' "
- Quoting TrueCrypt Developer David: "There is no longer interest."

The TrueCrypt Code:
- Really and Truly Lovely

The v7.1a -to- v7.2 Diff:
- https://gist.github.com/riverar/4052f4a792ad2b784f8f#file-gistfile1-diff-L2651

A comment from the 3rd blog post:
- DedRyzing (May 30, 2014 at 6:56 pm) says:
- Where TC excels is in it's being crossplatform across Linux, Mac and Win. It is sure nice to encrypt a USB drive, or file container, and be able to take it to any other system and read it. Not sure of any other free / open source solution that offers this. For full disk / volume encryption, I use other solutions, but for portable encryption, will continue using TC until such time there is a reason not to.

The Future:
- TrueCrypt.ch
- OpenCryptoAudit
- OpenCryptoAudit (@OpenCryptoAudit)
    - *Three Tweets:*
    - We are considering several scenarios, including potentially supporting a fork under appropriate free license, w/ a fully reproducible build.
    - More details on our work with the Critical Infrastructure Initiative: http://www.linuxfoundation.org/news-media/announcements/2014/05/core-infrastructure-initiative-announces-new-backers
    - We are continuing forward with formal cryptanalysis of TrueCrypt 7.1 as committed, and hope to deliver a final audit report in a few months.