Security Now! #527 - 09-29-15

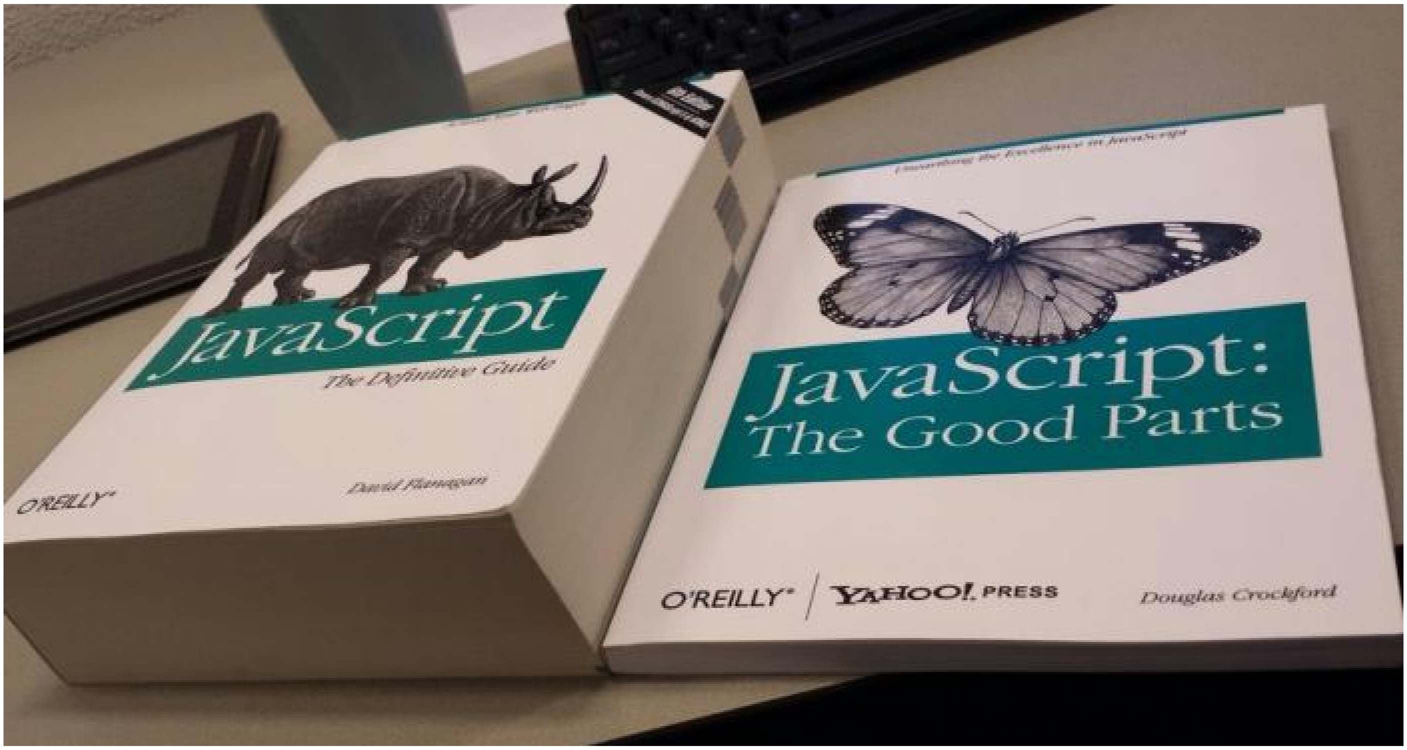
Q&A #219

- *“Takes a bending and keeps on sending!”*
- *“Alexa”...(pause)...”Tell me something I don’t know”*
- *Leo!!... welcome to the iMessage “Blue Balloon” society!*
- *Pill-Pack Sponsor: Vitamin D*

This week on Security Now!

- Probably time to migrate away from TrueCrypt
- Quick AdBlocker App Update
- Thinkpad is, sadly, no longer "clean."
- New concerns over AntiVirus add-on utilities

This, basically, says it all:



Security News:

After 16 months... It's time to gradually migrate away from TrueCrypt.

- James Forshaw, a member of Google's Project Zero team which regularly finds vulnerabilities in widely used software, recently discovered two vulnerabilities in the low-level kernel driver that TrueCrypt installs on Windows systems.
- Once again we have breathless, over-the-top headlines: "Newly found TrueCrypt flaw allows full system compromise" (whatever that actually means)
- Does it mean that your TrueCrypted encrypted data is now all vulnerable? No.
- <quote> ComputerWorld: The flaws, which were apparently missed in an earlier independent audit of the TrueCrypt source code, could allow attackers to obtain elevated privileges on a system if they have access to a limited user account.
- James Forshaw, who found the problems tweeted: though not added intentionally into the codebase, they are the type that could have slipped past a code audit and review.
- Threatpost: VeraCrypt Patched Against Two Critical TrueCrypt Flaws
  - https://threatpost.com/veracrypt-patched-against-two-critical-truecrypt-flaws/114833/
- Both vulnerabilities are considered critical, though one more than the other:
  - The issue is critical because any process can call a system driver, and a flaw has been found in the TrueCrypt driver which would allow a limited account to obtain admin privileges.
  - The second less critical vulnerability occurs because TrueCrypt does not properly validate the security context of the calling user. This could allow an attacker to impersonate another user on the same machine and allow them to dismount a TrueCrypt volume or change how the software is configured.
- The VeraCrypt folks said that they agree with James Forshaw, that the vulnerabilities were not intentionally introduced.
- Jeremy Collake / September 27, 2015 at 9:51 pm
  - At least these are local vulnerabilities - privilege escalation to be specific. Honestly, I haven't yet decided whether I should trust VeraCrypt over TrueCrypt's last encryption-enabled release. It's a tough call. Why was TrueCrypt really abandoned in the way it was? We may never know. We don't really even know who it's primary contributors were. Now VeraCrypt is here. Do we trust them, and it? If we trust by default, then they've given us no reason not to trust them. In contrast, if we are skeptical by default, they've not had enough time to earn our trust.

- Another poster, Tom Hawack / September 28, 2015 at 9:51 am
  - And what IF the true relationship between TrueCrypt and VeraCrypt was the reverse of what is officially mentioned?

    What if the truth was that the TrueCrypt developers had been pressured to modify their code to allow TrueCrypt volumes to be deciphered and that, with their refusal, a campaign was begun to discredit it with a more compliant VeraCrypt glorified as the solution?

    Nowadays nothing surprises me anymore. I'm neither cynical nor paranoid but we all know that when it comes to the ability to dig into one's secrets all attitudes can be imagined. Imagined only. I'm sticking on TrueCrypt for the time being, motivated by doubt not by convictions.

"Crystal" accepts Eyeo (E-I-E-I-O's) Acceptable Ads deal

- http://www.theverge.com/2015/9/24/9393941/clear-ios-ad-blocker-offering-paid-whitelist
- Extortion? Compromise? Tough call...
- Dean Murphy will receive a flat monthly fee from Eyeo for enabling ABP's whitelist by default.
- Dean told the Wall Street Journal: "Given how popular Crystal has become, it doesn't provide any way for users to support publishers. I decided that's a good feature to provide, and from what I've seen the 'acceptable ads' policy doesn't let through what I would classify as bad ads."

- Dissenting opinions:
  - Matt Buchanan writing for "The Awl" website: "If your adblocker takes money from you in order to block ads, and then takes money from huge companies in order to show you the ads that you paid for it to block, then yes; it's just using you to erect a tollbooth."
  - http://www.theawl.com/2015/09/probably

- Advertising Age / Ad Blocking: The Unnecessary Internet Apocalypse
  The Ad Industry Needs to Disrupt the Disruptors
  - http://adage.com/article/digitalnext/ad-blocking-unnecessary-internet-apocalypse/300470/
  - Randall Rothenberg, the president and CEO of the Interactive Advertising Bureau, the trade association for interactive marketing in the U.S.

    <quote> The digital marketing and media industry regularly confronts fresh adversaries eager to intercept the flow of ad dollars, often to the disadvantage of consumer choice. Ad blocking is the latest crisis du jour, a potentially existential threat to the industry. To combat it effectively, it's essential to distinguish ad blocking's two sources -- and their significance.

    As abetted by for-profit technology companies, ad blocking is robbery, plain and simple -- an extortionist scheme that exploits consumer disaffection and risks distorting the economics of democratic capitalism. When implemented by consumers, ad blocking is a crucial wakeup call to brands and all that serve them about their abuse of consumers' good will.
- IAB holding a press conference today...

Ad Blockers have dropped from the top spots in the App Store

- Our pick for the best "no brainer" blocker, Purify, is holding at #3.
- The others have dropped way down:
  - "Crystal" is at #21
  - "Blockr" is not in the top 150.
  - "1Blocker" -- performance winner with high-end controls nowhere to be found
- "Peace" refunded $3 to all purchasers... but still usable.

ThinkPads are phoning home too...

- Michael Horowitz, ComputerWorld's Defensive Computing columnist
    - http://www.computerworld.com/article/2984889/windows-pcs/lenovo-collects-usage-data-on-thinkpad-thinkcentre-and-thinkstation-pcs.html
    - <quote> On a recent edition of the Security Now podcast, Steve Gibson read a note from a listener saying that while Lenovo was corrupting their consumer PCs, [Lenovo] have kept their hands off the ThinkPad line. Both Gibson and the show host, Leo Laporte, proceeded to sing the praises of ThinkPads.

      But there's more to the story.
- Recently purchased two newly refurbished ThinkPads from IBM a T520 and a T420.
- Using Nirsoft's very nice "TaskSchedulerView" utility.
- https://support.lenovo.com/us/en/documents/ht102023
- http://www.makeuseof.com/tag/now-three-pre-installed-malwares-lenovo-laptops/
- Lenovo: Lenovo systems may include software components that communicate with servers on the internet - All ThinkCentre, All ThinkStation, All ThinkPad
- On "Think" brand products, Lenovo collects 2 types of data:
    - Application usage data (metrics)
    - Preloaded application inventory data

A/V can weaken, more than strengthen, a system's security

- Security wares like Kaspersky AV can make you more vulnerable to attacks.
- Products often open computers to hacks they otherwise wouldn't be vulnerable to.
- Antivirus applications and other security software are supposed to make users more secure, but a growing body of research shows that they can open people to hacks they otherwise wouldn't be vulnerable to.
- The latest example is antivirus and security software from Kaspersky Lab.
- Tavis Ormandy, a member of Google's Project Zero vulnerability research team, recently analyzed Kaspersky's AV and quickly found a raft of easy-to-exploit bugs that made it possible to remotely execute malicious code on the underlying computers.
- Kaspersky has fixed many of the bugs and is in the process of repairing the remaining ones.
- In a blog post published last Tuesday, Tavis said it's likely he's not the only one to know of such "game-over" vulnerabilities.
    - Tavis wrote: "We have strong evidence that an active black market trade in antivirus exploits exists," he wrote, referring to recent revelations that hacked exploit seller Hacking Team sold weaponized attacks targeting antivirus software from Eset.
    - He continued: "Research shows that security and A/V is an easily accessible attack surface that dramatically increases exposure to targeted attacks. For this reason, the vendors of security products have a responsibility to uphold the highest secure development standards possible to minimize the potential for harm caused by their software. Ignoring the question of effectiveness, attempting to reduce one’s exposure to opportunistic malware should not result in an increased exposure to targeted attacks."
- Kaspersky is not alone... similar problems have also been found in products from FireEye, Sophos, and Eset.

SpinRite:

From: "Name Withheld" <withheld@sorry.about-that>
Subject: How SpinRite Saved the Plane
Date: Fri, 25 Sep 2015 07:02:14 -0000
X-Location: Earth, The Universe

How SpinRite saved the plane!

Dear Mr Steve,

- Please note that some details in this story have been changed to protect my identity, which is quite important as you'll soon find out. I am a senior IT director at an airline that shall remain unnamed, but I did not land this role overnight, I worked my way up, all the way from tech support. Naturally I still have the gift-of-geek in me and always carry around several USB drives and some mini CDs (8cm ones) full of Linux distros and troubleshooting tools.

On a recent international flight, just before takeoff I noticed that the crew were having trouble with the IFE (in-flight-entertainment) system, every time the media library was loaded it stopped and the system rebooted. After a couple of tries they disabled output to the passenger screens, but I knew that they were having some HDD trouble.

I deliberated what to do, because even as IT director I cannot touch the IFE without authorization. Access is highly restricted, and only senior technicians on the ground have root access, the crew can only use the built-in troubleshooting tools. But after the seat-belt signs turned off, I promptly introduced myself to the co-pilot (who was taking a stroll through the plane), showed him my ID and badge, and offered to help. He was surprised and said he'd contact ground and get back to me.

So I waited... 10 minutes later I get a note from the captain authorizing me to try and fix the IFE.

/* The following is not for public knowledge. <<Steve cut this out of the posted show notes>> It discussed security details. */

I popped in my SpinRite bootable USB (corporate license), and since we were in a rush, with the passengers getting grumpy, I only did a quick scan on level 2. At about 11 percent, SpinRite found and fixed quite a few sectors of the media drive, and when it got to 30% cruising along with no additional errors being found, I decided to stop it and try my luck.

There was a jubilant outcry when the FML (flight-media-library) loaded without a hitch and to the passengers and my delight we could continue to enjoy the flight (of which we still had 9 hours).

So allow me to express my sincerest thanks for you and your marvelous product, you shall be blessed hundredfold and live long and prosper!

Name Withheld (due to possible breach of protocol)