Security Now! #528 - 10-06-15

Breaches & Vigilante Worms

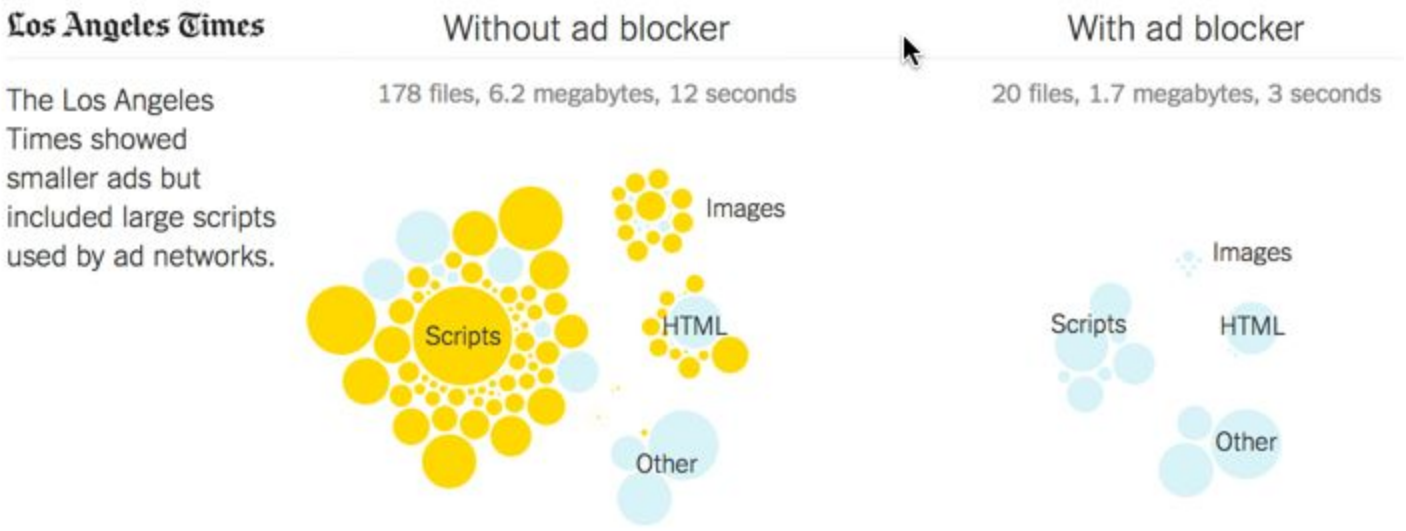
- Video game violence … and VR??

This week on Security Now!

- Breaches at Patreon, Experian & Scottrade
- Stagefright 2
- Router Vigilante Worm
- Problems with VeraCrypt
- A bunch of follow-ups and minor notes
- Security implications of the VW trick
- Android Marshmallow's major security improvements

Carriers are Making More From Mobile Ads than Publishers Are

Consumers pay 16.6x more in data costs than
top 50 news sites are making in ad revenue



Security News:

Patreon

- Jack Conte, CEO/Co-founder:
- Here are some technical details of the incident:
  - The unauthorized access was confirmed to have taken place on September 28th via a debug version of our website that was visible to the public. Once we identified this, we shut down the server and moved all of our non-production servers behind our firewall.
  - There was no unauthorized access of our production servers. The development server included a snapshot of our production database, which included encrypted data.
  - The development server did not have any private keys that would allow login access to any other server. We verified our authorization logs on our production servers to ensure that there was not any unauthorized access.
  - As a precaution, we have rotated our private keys and API keys that would allow access to third-party services that we use.
  - We protect our users' passwords with a hashing scheme called 'bcrypt' and randomly salt each individual password. Bcrypt is non-reversible, so passwords cannot be "decrypted." We do not store plaintext passwords anywhere.
- Hackers have published nearly 15 GB of password data, donation records, and source code taken from Patreon's development server.
- Security researcher Troy Hunt (who maintains the "Have I been Pwned?" website) has downloaded, examined, and verified that it's Patreon's data.
  - Troy: "The amount and type of data posted by the hackers suggest the breach was more extensive and potentially damaging to users than was previously assumed."
  - Troy has sifted through the database and found 2.3 million unique eMail addresses, including his own.
  - Troy wrote:
    - "You can determine how much those using Patreon are making."
    - "Everything private is now public."
  - https://haveibeenpwned.com/
  - Five days before, Swedish security firm "Detectify" notified Patreon of the trouble.
    - Shodan (https://www.shodan.io/) can be searched for server details, and the server at "zach.patreon.com" was replying with the header: "Server: Werkzeug/8.9.6 Python/3.4.0
    - http://labs.detectify.com/post/130332638391/how-patreon-got-hacked-publicly-exposed-werkzeug
- Werkzeug Utility Library
  - http://werkzeug.pocoo.org/
  - A very powerful library of Python utilities.
  - "In the Box"
    - HTTP header parsing and dumping
    - Easy to use request and response objects
    - Interactive JavaScript based in-browser debugger
    - 100% WSGI 1.0 compatible
    - Supports Python 2.6, 2.7 and 3.3.

        - Unicode support
        - Basic session and signed cookie support
        - URI and IRI utilities with unicode awareness
        - builtin library of fixes for buggy WSGI servers and browsers
        - integrated routing system for matching URLs to endpoints and vice versa
- The Werkzeug debugger allows visitors to execute code of their choice from within the browser. Werkzeug developers have long been clear about this capability and the massive risks that stem from using it in production environments.
- A secret key must be used to manually invoke the site debugger...
- But by triggering a bug on the site, the Werkzeug debugger would also be invoked.

T-Mobile/Experian

- The credit applications of 15 Million T-Mobile customers were stolen from the credit reporting agency, Experian... resulting in the complete identity theft of 15 million people.
- T-Mobile subcontracted is customer credit management to Experian.
- Experian -> "Experian North America today announced that one of its business units...experienced an unauthorized acquisition of information from a server that contained data on behalf of...T-Mobile, USA, Inc. The data included personally identifiable information for approximately 15 million consumers in the US, including those who applied for T-Mobile USA postpaid services or device financing from September 1, 2013 through September 16, 2015, based on Experian's investigation to date."
- [con't] "The data acquired included names, dates of birth, addresses, telephone numbers and Social Security numbers and/or an alternative form of ID like a drivers' license number, as well as additional information used in T-Mobile's own credit assessment."
- Experian is offering affected consumers two years of free credit monitoring through a service they own: "ProtectMyID.com"
    - But there's no expiration date on the stolen data.
    - Bad guys could easily wait two years... then leverage the data.
- Credit Card numbers can be changed, but Social Security Numbers, Dates of Birth, and drivers license numbers are identity theives' dream data. And they got 15 million sets.
- ADVICE? --> Initiate an immediate credit freeze with all three bureau.
    - With credit frozen, no new credit will be granted.
    - http://credit.about.com/od/privacyconcerns/qt/securityfreeze.htm
    - http://www.clarkhoward.com/credit-freeze-and-thaw-guide
    - http://www.creditcards.com/credit-card-news/credit-report-freeze-1282.php
    - http://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

Scottrade reports a data breach

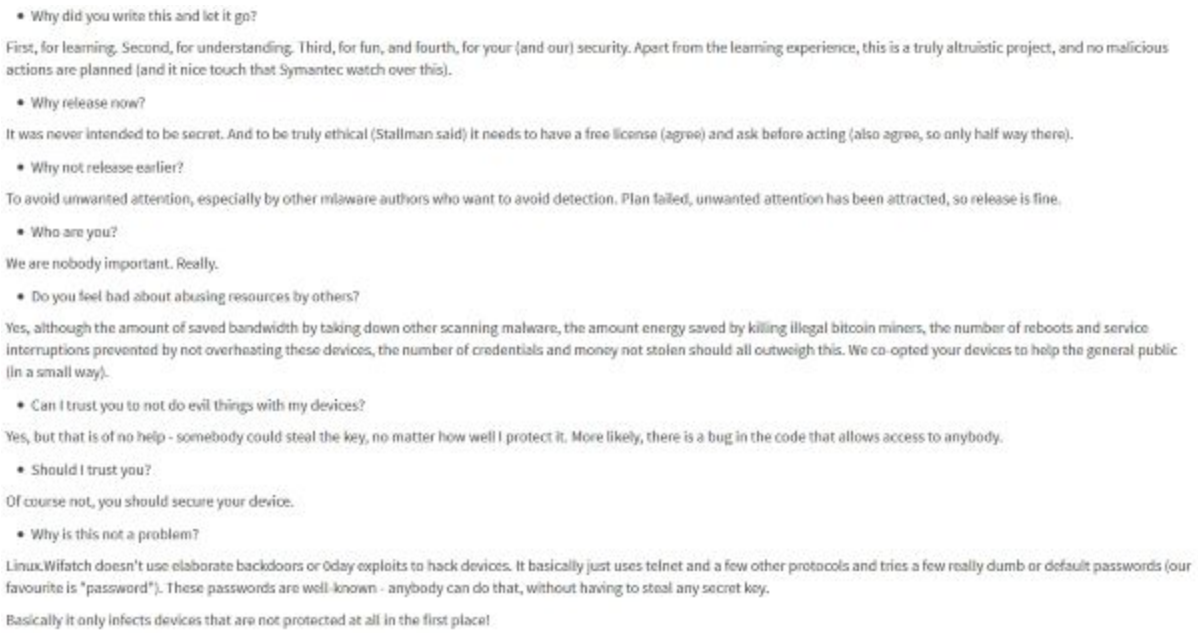
- https://about.scottrade.com/updates/cybersecurity.html
- 4.6 million customers
- Names, addresses, Social Security numbers, and other personal information
- Anyone with an existing Scottrade account prior to February 2014.
- ... the data breach took place over several months between late 2013 and early 2014!
- Login information and the trading platform were NOT affected.
- Perhaps just social engineering attacks against Scottrade customers.

Stagefight 2

- 15 CRITICAL Remote code execution vulnerabilities in LibStageFright.
- https://groups.google.com/forum/#!topic/android-security-updates/_Rm-IKnS2M8
- Affects all versions of Android since 2010.
- Oct 5th: Nexus OTA udpate
- Partners notified: Sept. 10th or earlier
- Google: The most severe of these issues is a Critical security vulnerability that could enable remote code execution on an affected device through multiple methods such as email, web browsing, and MMS when processing media files.

  We have had no reports of active customer exploitation of these newly reported issues. Refer to the Mitigations section for details on the Android security platform protections and service protections such as SafetyNet, which improve the security of the Android platform. We encourage all customers to accept these updates to their devices.
- "Linux.Wifatch" -- the IoT Vigilante Worm!
  - Symantec writes…

    Let me introduce you to Linux.Wifatch, one of the latest pieces of code infecting Internet of Things (IoT) devices. We first heard of Wifatch back in 2014, when an independent security researcher noticed something unusual happening on his home router. The researcher identified running processes that didn't seem to be part of the legitimate router software and decided to investigate further. During his analysis he discovered a sophisticated piece of code that had turned his home router into a zombie connected to a peer-to-peer network of infected devices.
  - What does it do?
    - Behaves just like a worm... scanning, finding, and "infecting" vulnerable routers.
    - Remains hidden
    - Coordinates actions through a peer-to-peer network
    - No malicious payloads
    - Hardens the security of its host devices
    - Kills any running Telnet daemon.
    - Keeping other viruses out by staying current on router vulnerabilities through its peer-to-peer network
    - Removes any pre-existing malware discovered
    - Patches up the router to cut off other channels of entry.
    - The code could have easily been obfuscated, but the author chose not to.
  - The source code contains a copy of Richard Stallman's eMail signature: "To any NSA or FBI agents reading this: please consider whether defending the US constitution against all enemies, foreign or domestic, requires you to follow Snowden's example."
  - Symantec estimates that 10's of thousands of devices are infected.
    - Mostly in China, Brazil, Mexico, India, Vietnam, Italy, Turkey
  - Yesterday... Wifatch's author posted a reply to Symantec's blog…



- Why did you write this and let it go?

First, for learning. Second, for understanding. Third, for fun, and fourth, for your (and our) security. Apart from the learning experience, this is a truly altruistic project, and no malicious actions are planned (and it nice touch that Symantec watch over this).

- Why release now?

It was never intended to be secret. And to be truly ethical (Stallman said) it needs to have a free license (agree) and ask before acting (also agree, so only half way there).

- Why not release earlier?

To avoid unwanted attention, especially by other mlaware authors who want to avoid detection. Plan failed, unwanted attention has been attracted, so release is fine.

- Who are you?

We are nobody important. Really.

- Do you feel bad about abusing resources by others?

Yes, although the amount of saved bandwidth by taking down other scanning malware, the amount energy saved by killing illegal bitcoin miners, the number of reboots and service interruptions prevented by not overheating these devices, the number of credentials and money not stolen should all outweigh this. We co-opted your devices to help the general public (in a small way).

- Can I trust you to not do evil things with my devices?

Yes, but that is of no help - somebody could steal the key, no matter how well I protect it. More likely, there is a bug in the code that allows access to anybody.

- Should I trust you?

Of course not, you should secure your device.

- Why is this not a problem?

Linux.Wifatch doesn't use elaborate backdoors or 0day exploits to hack devices. It basically just uses telnet and a few other protocols and tries a few really dumb or default passwords (our favourite is "password"). These passwords are well-known - anybody can do that, without having to steal any secret key.

Basically it only infects devices that are not protected at all in the first place!

Follow-up on HOLA

- http://arstechnica.com/security/2015/06/hola-vpn-used-to-perform-ddos-attacks-violate-user-privacy/
- HOLA is dangerously insecure.
- Allows for remote code execution.
- Hola sells access freely and allows the network to be used maliciously.
- >>> Increased Attack Surface <<<
- http://adios-hola.org/

Problems with VeraCrypt

- v1.15 has acknowledged file and directory deletion problems.
- Dave DeBruce, last Thurs Oct 1st...
- https://www.grc.com/groups/securitynow:28120
- I have been a long time TrueCrypt user but because of SN527 I decided to give Veracrypt a try.

  I am on Win 7 Pro 64bit. It installed fine alongside of Truecrypt as they do not bump into each other at all. It was able to mount my truecrypt volume fine. I mounted both a new .hc volume and my old .tc volume. Copied all over to veracrypt and thought all was fine but there are issues.

  With 1.15 you can delete files from the volume but not directories. You get an error saying the drive letter cannot be found. I am sure this will be fixed but it looks like I stay with truecrypt for now.

  This is a known and reported issue to the veracrypt folks but it is a big enough issue where I cannot use it like this. Anyone else try this and have any issues?

F-Secure jumps into the iOS AdBlocking game

- https://www.f-secure.com/en_US/web/home_us/adblocker
- https://itunes.apple.com/app/f-secure-adblocker/id1040899919
- But... no Whitelisting option. :(

Verisign launched a free public DNS service:

- http://www.verisign.com/en_US/innovation/public-dns/index.xhtml
- http://blogs.verisign.com/blog/entry/introducing_verisign_public_dns_a
- <quote> Why choose Verisign Public DNS?
  - Stability: Confidence in a highly reliable public DNS platform
  - Security: Robust protection from security flaws
  - Privacy: Assurance that your public DNS data will not be sold to third parties
- IP: 64.6.64.6 & 64.6.65.6

Carriers are Making More From Mobile Ads than Publishers Are

- Consumers pay 16.6x more in data costs than top 50 news sites are making in ad revenue
- Rob Leathern: https://medium.com/@robleathern/carriers-are-making-more-from-mobile-ads-than-publishers-are-d5d3c0827b39

Foobytes.com via Christy Ramsey @christyramsey

- .@SGgrc Example of a "please unblock our ads" popup at fossbytes.com (while using uBlock Origin)
- <bold>Please consider reading this notice.</bold>
  We've found out that you are using AdBlock Plus or some other adblocking software which is preventing the page from fully loading.

  We don't have any disturbing banner, Flash, animation, obnoxious sound, or popup ad. We do not implement these annoying types of ads!

  We need money to operate the site, and almost all of it comes from our online advertising. And currently we are running low on budget.

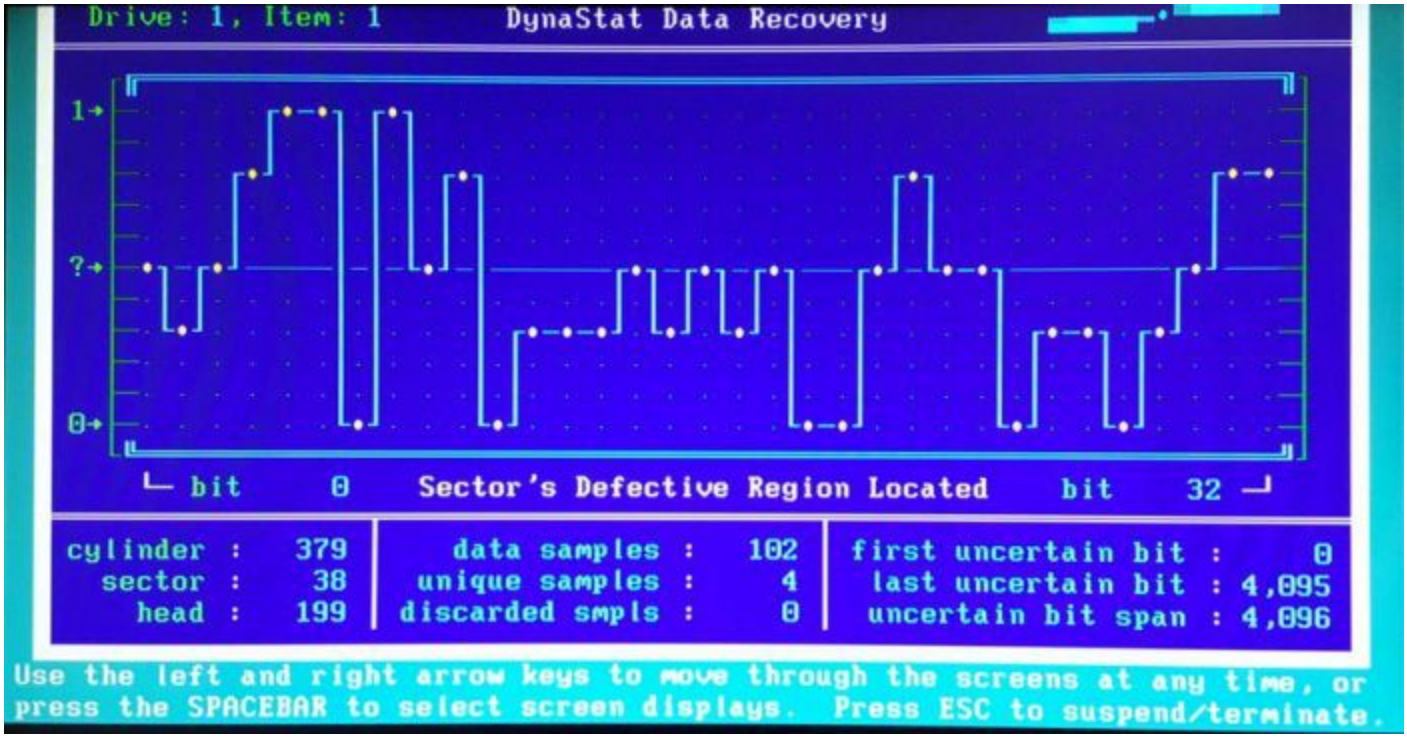
  Please add fossbytes.com to your ad blocking whitelist or disable your adblocking software.
- (1.7 Mb vs 2.2 Mb 20% load time increase.)

Edward Snowden:

- Now with 1,364,840 followers and in 7,191 lists.
- Following exactly 1: @NSAGov

SpinRite:

Anthony Gladden @Anthony_Gladden Saturday, October 3rd @ 6:12pm
SpinRite saving my ass..ets once again. Thank you!



Too much reliance upon SpinRite??

More Security News:

Android Marshmallow's 10 best new security features

- Boot Verification
    - Catching up with Chromebook, Marshmallow implements boot verification to warn users that the core software might have been interfered with or corrupted during the boot process.
    - YELLOW - an unknown OS has been loaded: "Your device has loaded a different operating system."
    - ORANGE - the bootloader is not locked: "Your device software cannot be checked for corruption. Please lock the bootloader."
    - RED - the boot image is corrupted: "Your device is corrupt. It cannot be trusted and may not work properly."

- More control and visibility into app permissions:
    - Users can now agree to app permissions as they are needed rather than as a long list when software is installed.
    - Users can also examine all apps which have been granted a given permission.
    - But... apps need to support this operation through new APIs.

- "Smart Lock" for passwords
  - "Allow the passwords of your apps and websites to be saved to your Google account. When disabled, no passwords will be saved or returned from this account.
  - So this is a new capability to store third-party passwords in a user's Google account. Again... requires new API to be supported.

- Encryption Enabled by Default
  - Use of low-level hardware should minimize the performance impact of FDE (full disk encryption).
  - Despite bad publicity for Google over the Nexus 6 smartphone stuttering when enabling full-disk encryption (FDE), the first devices running Android M, the 5X and 6P, have encryption turned on by default. The underlying hardware should support this with no performance issues. The assumption is that all other manufacturers will have to follow suit with default encryption on Android M devices.

- Better clarity into VPN configuration and usage - for BYOD
  - Settings -> More -> VPN.
  - Specific VPN services and Apps now appear for configuration under the Settings > More > VPN tab.

- "Nexus Imprint" integrated fingerprint authentication
  - Previously, individual phone makers had to integrate fingerprint support themselves.
  - Marshmallow now offers a new fingerprint authentication API.
  - Branded 'Nexus Imprint' (for new Nexus devices at least), this will allow users to lock and unlock devices with a finger scan and might encourage more vendors to add them.

- Integrated auto application data backup
  - A mechanism for apps to back up to 25MB of individual settings data (for example, gameplay state) so that users reinstalling the app later on don't return to zero.

- Voice control without unlocking the phone
  - Not an obvious security feature, but from the lock screen users will now be able to perform actions such as search without having to unlock the phone into an insecure state.

- Android Security Patch Level
  - Clearly provides the date at which the last security update was applied.
  - The regular patching applies to all Google-controlled Nexus devices, but so far the Android M devices are the only ones that show this information. In future, Android users should known precisely where they are in the update timeline.

- Flexible Secure Storage
  - Following on from encryption by default, Android M devices will automatically extend app store on to SD cards without that having to be done manually. This storage will also be encrypted. Not a security feature but a secure implementation of a new feature that shows how things have changed.

What the VW discovery means for the encryption software industry

- Nadim Kobeissi
    - https://nadim.computer/2015/09/25/volkswagen-backdoor.html

- Context Aware Security (CAS)