Security Now! #526 - 09-22-15

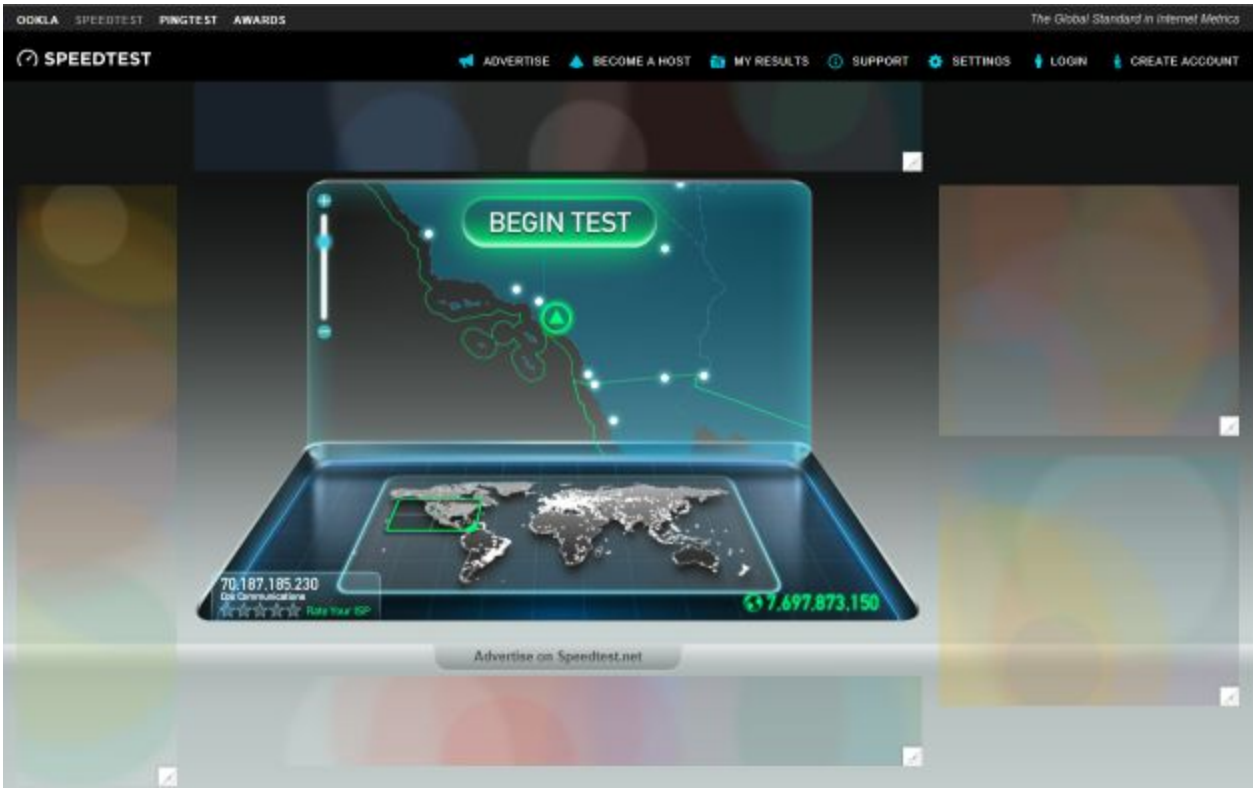
iOS Content Filters

"Takes a bending and keeps on sending!"

This week on Security Now!

- iOS XcodeGhost
- Critical Adobe FLASH update
- AVG's privacy policy update
- Cisco routers "implanted"
- Ashley Madison password mystery
- VW/Audi caught red handed?
- India's encryption trial balloon
- Stagefright update update
- Miscellany and Discussion of initial AdBlocking offerings

My use of Speedtest.net surrounded by and supported by Google Contributor:



Security News:

iOS XcodeGhost

- Initially discovered by a Chinese developer:
  - On a popular Chinese forum V2EX, a user "realpg" mentioned his experience when developing an iOS app. In the discussion, "realpg" said that when they were developing a very simple iOS app that had no Internet functionality and didn't use any iCloud APIs. But the app would frequently display a dialog to ask the developer to input his iCloud password. They tested the app in their special testing iPhone without jailbreak. Then they captured the network traffic and discovered communication with a remote Command and Control server.

    Based on "realpg"'s account of the events, we believe that stealing passwords or potentially exploiting vulnerabilities in iOS and in legitimate applications may be XcodeGhost's purpose.

- Palo Alto Networks found 39 infected apps.
  - Establishes a connection to remote command & control servers.
  - Sends device and app information.
  - Can receive commands to:
    - Prompt a fake alert dialog to phish user credentials
    - Hijack URL schemes to obtain control.
    - Read and write data in the user's clipboard.
  - Launch phishing attacks to obtain iCloud passwords.

- The Chinese online security company Qihoo said it has found more than 300 infected apps.
- Xcode is the "tool chain" suite of tools used to developer Apps.
- Bad versions of Xcode were all on a cloud hosting service owned by the Chinese Internet company Baidu. Baidu has removed them.
- Once infected apps are downloaded the malicious code can open websites designed to further infect the devices. The code can also open innocuous-looking pop-up screens that ask users for more information, like passwords to their Apple account. Since the dialogue is a prompt from the running application, the victim may trust it and input a password without suspecting foul play.
- Two factors:
  - Hackers did not crack Apple's software. They took advantage of the fact that many Chinese developers use copies of Xcode that are held on Chinese servers, since they load faster than the version of the code that's available from Apple.
  - The bad Xcode could only be used by developers who had disabled Apple's safety features. Otherwise Apple would have presented a warning that something was wrong with Xcode.
- Many of the websites that were receiving stolen information have been discovered and shut down, according to researchers.

iOS9 -- also brought a TON of security improvements and tweaks

- Security Content of iOS9
- https://support.apple.com/en-us/HT205212

Adobe Flash Update

- Critical software update fixes nearly two dozen vulnerabilities
- Now at v19.0.0.185 for Windows & Mac.
- Chrome and IE manage Flash on their own and both are at the same level.
- Firefox:
    - Tools / AddOns / PlugIns
    - Link at the top: "Check to see if your plugins are up to date"
    - Set: "Ask to Activate"

AVG to begin selling browsing and search history to advertisers...

- http://www.wired.co.uk/news/archive/2015-09/17/avg-privacy-policy-browser-search-data
- In a few weeks (October 15) AVG's updated privacy policy goes into effect.
- The new policy has raised hackles within the privacy community because it states that users of the AVG anti-virus will be implicitly permitting AVG to sell search and browser history data to third-party advertisers in order to "make money" from its antivirus software.
- The trouble is that Antivirus software runs with elevated privileges so it can detect and block malware, adware, spyware and other threats. And AVG is one of the A/V suites that installs its own root certificate into our machines -- a la Superfish -- allowing it to intercept, decrypt, and inspect ALL web browser traffic.
- In response to the uproar…
    - An AVG spokesperson explained that any non-personal data it collected and sold to advertisers would be cleaned and anonymised, making it impossible to link it back to individual users. "Many companies do this type of collection every day and do not tell their users," the spokesperson said.
- But... if that data is disconnected from the user, how then could it be of any value to the advertiser?
    - Answer: It *must* be tied to existing tracking cookies so that advertisers essentially have an agent installed in end user machines which can see, collect, and report on everything.
    - (It's a nice job if you can get it!)

Cisco routers in at least 4 countries infected by highly stealthy backdoor

More than a dozen routers in four countries infected with fully featured implants.

- http://arstechnica.com/security/2015/09/attackers-install-highly-stealthy-backdoors-in-cisco-routers
- Researchers at FireEye have discovered "SYNful Knock" malware "implants" (NSA term) on 14 routers in Ukraine, the Philippines, Mexico and India.
- FireEye said: The feat can only be achieved by a handful of nation-state actors.
- Details:

- The implant consists of a modified Cisco IOS image that allows the attacker to load different functional modules from the anonymity of the internet. The implant provides unrestricted access using a secret backdoor password. Each of the modules are enabled via the HTTP protocol (not HTTPS), using a specifically crafted TCP packet sent to the router's interface. The packets have a nonstandard sequence and corresponding acknowledgment numbers. The modules may manifest either as independent executable code or hooks within the routers IOS to provide functionality similar to a backdoor password. The backdoor password provides access to the router through the console and Telnet.
- The "implant" resides within the Cisco router's non-volatile firmware.
- Full FireEye Report: https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html

Once seen as bulletproof, 11 million+ Ashley Madison passwords already cracked

Programming errors make 15.26 million accounts orders of magnitude faster to crack.

- http://arstechnica.com/security/2015/09/once-seen-as-bulletproof-11-million-ashley-madison-passwords-already-cracked/
- A total of 36 million passwords
- All were protected by a strong 4,096 iteration Bcrypt PBKDF... making the cracking all but impossible.
- But 15.26 million of the accounts also had something else: An MD5 token.
- The MD5 token was one of:
  - MD5(Lowercase(username - available in plaintext)'+'::'+Lowercase(password))
  - MD5(Lowercase(user name + e-mail address + plaintext password + "73@^bhhs&#@&^@8@*$")

VW & Audi recall

- http://tech.slashdot.org/story/15/09/18/1745221/volkswagen-ordered-to-recall-500k-vehicles-over-its-own-malicious-programming
- EPA, California Notify Volkswagen of Clean Air Act Violations
  - http://yosemite.epa.gov/opa/admpress.nsf/0/DFC8E33B5AB162B985257EC40057813B
  - Washington - Today, EPA is issuing a notice of violation (NOV) of the Clean Air Act (CAA) to Volkswagen AG, Audi AG, and Volkswagen Group of America, Inc. (collectively referred to as Volkswagen). The NOV alleges that four-cylinder Volkswagen and Audi diesel cars from model years 2009-2015 include software that circumvents EPA emissions standards for certain air pollutants. California is separately issuing an In-Use Compliance letter to Volkswagen, and EPA and the California Air Resources Board (CARB) have both initiated investigations based on Volkswagen's alleged actions.

    As described in the NOV, a sophisticated software algorithm on certain Volkswagen vehicles detects when the car is undergoing official emissions testing, and turns full emissions controls on only during the test. The effectiveness of these vehicles' pollution emissions control devices is greatly reduced during all normal driving situations. This results in cars that meet emissions standards in the laboratory or testing station, but during normal operation, emit nitrogen oxides, or

NOx, at up to 40 times the standard. The software produced by Volkswagen is a "defeat device," as defined by the Clean Air Act.

- Affected diesel models include:
  - Jetta (Model Years 2009 – 2015)
  - Beetle (Model Years 2009 – 2015)
  - Audi A3 (Model Years 2009 – 2015)
  - Golf (Model Years 2009 – 2015)
  - Passat (Model Years 2014-2015)

- Commentary
  - http://www.cleanmpg.com/forums/showthread.php?t=52425
  - Just when the promise of Diesel was gaining new legs thanks to lower diesel fuel prices, new low carbon fuels and engines that could easily meet the strictest emissions standards in the world, the EPA issued a Notice of Violation (NOV) letter to the largest seller of diesel engines in the U.S. and the largest auto manufacturer in the world.

    During dynamometer testing for both Emissions and Fuel Economy certification, 2.0L VW TDIs from 2009 – 2015 worked in a "Dyno-Mode" tune that performed satisfactorily and easily met the legal limits for a variety of pollutants including NOx.

    Unfortunately when the ECU detected that the car was not on a dynamometer – I am still not entirely clear as to how this was accomplished – the emissions controls were allowed to relax providing both the power and efficiency TDI owners have come to rely on. This in turn allowed between 10 and 40 times the legal limit of NOx to be emitted while driven in the manner that we all drive.

    In an EPA teleconference call with media, Cynthia Giles, an enforcement officer at the EPA stated, "Put simply, these cars contained software that turns off emissions controls when driving normally and turns them on when the car is undergoing an emissions test."

    The "Defeat Device" or "Dyno-Mode" programming within the Bosch EDC17 ECU has been a part of OEM testing for decades. It was the relaxing of the emissions control systems code that caused the real problems.

India's Draft National Encryption Policy

- https://publicintelligence.net/india-draft-encryption-policy/
- The following draft copy of the National Encryption Policy was released for public comment by the India Department of Electronics and Information Technology. The policy has been widely criticized for requiring businesses, internet service providers and even private citizens to store decrypted versions of encrypted communications for 90 days to provide to the government and law enforcement. An article in the Times of India dated September 20, 2015 quotes Pranesh Prakash, policy director at the Bengaluru-based Center for Internet and Society, who describes the draft policy as a "bad idea conceived by people

who do not understand encryption."

- https://info.publicintelligence.net/IN-DraftEncryptionPolicy.pdf
- <quote>
  The recognition of the need to protect privacy and increase the security of the Internet and associated information systems have resulted in the development of policies that favour the spread of encryption worldwide. The Information Technology Act 2000 provides for prescribing modes or methods for encryption (Section 84A) and for decryption (Section 69). Taking into account the need to protect information assets, international trends and concerns of national security, the cryptographic policy for domestic use supports the broad use of cryptography in ways that facilitates individual / businesses privacy, international economic competitiveness in all sectors including Government.

  This policy is not applicable to sensitive departments / agencies of the government designated for performing sensitive and strategic roles. This policy is applicable to all Central and State Government Departments (including sensitive Departments / Agencies while performing non-strategic & non-operational role), all statutory organizations, executive bodies, business and commercial establishments, including public sector undertakings and academic institutions and all citizens (including Personnel of Government / Business performing non-official / personal functions).

- Objectives:
  <quote> To synchronize with the emerging global digital economy / network society and use of Encryption for ensuring the Security / confidentiality of data and to protect privacy in information and communication infrastructure without unduly affecting public safety and National Security.

- Basically: Full regulation of all use of encryption within India's borders.
- Government dictates allowable encryption algorithms and key lengths.
- Applies to data-in-transit and data at rest.
- Key concept: Plaintext must be produceable, upon demand, for anything encrypted within the past 90 days.

- <quote>
  On demand, the user shall be able to reproduce the same Plain text and encrypted text pairs using the software / hardware used to produce the encrypted text from the given plain text. Such plain text information shall be stored by the user/organisation/agency for 90 days from the date of transaction and made available to Law Enforcement Agencies as and when demanded in line with the provisions of the laws of the country.

- In case of communication with foreign entity, the responsibility of providing readable plain-text along with the corresponding Encrypted information shall rest on entity located in India.

- Service Providers located within or outside India, using Encryption technology for providing any type of services in India, must enter into an agreement with the Government for providing such services in India.

- Only the algorithms and key sizes for Encryption, as notified under the provisions in this Policy, will be used by all categories of users.

- Mechanics:
    - All vendors of encryption products shall register their products with the designated agency of the Government. While seeking registration, the vendors shall submit working copies of the encryption software / hardware to the Government along with professional quality documentation, test suites and execution platform environments. The vendors shall work with the designated Government Agencies in security evaluation of their encryption products. Complete confidentiality will be maintained in respect of information shared by the vendors with designated agency. The vendors shall renew their registration as and when their products are upgraded.

    - The Government will notify the list of registered encryption products from time to time, without taking responsibility for security claims made by the vendors.

    - The vendors of encryption products or service providers offering encryption services shall necessarily register their products / services with Government for conducting business in the country.

    - Encryption products may be exported, but with prior intimation to the designated agency of Government of India.

    - Users in India are allowed to use only the products registered in India.

Stagefright fixes are continuing to drift out into devices.

LetsEncrypt - via Twitter: Simon @sphere_au
- Just got @letsencrypt working on my webserver, thanks to @jdkasten on the support forums for ironing out a config issue quickly. (ping @SGgrc)

Miscellany:

Leo's battery advice on iOS Today:
- 100% correct!
- Battery University advice -- don't leave device plugged in overnight?
- Only plug it in enough to charge
- Don't charge it to 100%

Peter Hamilton's "The Chronicle of the Fallers"
- The Abyss Beyond Dreams (2014)
- The Night Without Stars...

SpinRite:

Jim Gerry in League City, TX
Mr. Gibson,

I have been a loyal customer for a LONG time. How long? I was digging around my closet and found an old "SpinRite: A Guide for Owners, Version 1.2", and that's what prompted me to write this email.

I just wanted to say, "Thank you!" I have used one version of your software on every hard drive I've ever owned, going all the way back to my 10 MB HDD on my IBM PC/XT. I cannot tell you how many HDDs I've owned over the years, but your software was used to rescue my data, time and time again, after the drives inevitably quit booting. It was always easier to recover my HDD with SpinRite than to restore from backups!

Your software is as relevant today as it was in the 1980s! Simply amazing!

---

iOS Content Filtering & Blocking

Dave Winer / Scripting News / Saturday, Sept 19th:
(We previously noted Dave grumbling about OSX suddenly becoming overly social, offering its opinion and seeming less and less like a simple (and silent) obedient tool.)
http://scripting.com/2015/09/19/advertisingIsUnwanted.html
<Quote>
I think of advertising as "unwanted commercial messages."#

The unwanted part is key. I do a lot of seeking of commercial information using the web. We all do, all the time. That's how business works on the web.#

It seems to me that news orgs have to figure out how to make people come to their sites seeking commercial information. They are in the information gathering business after all. Let some of the information you seek pertain to me spending money wisely or in fun or gratifying ways. #

What if I could go to my local paper to buy a house. I'm always interested in buying real estate. If they sold me a house, then they would make money from the sale. A lot more than a few cents they make off me every year for the ads I ignore. #

Maybe not a house. How about Internet connectivity. Or a movie date. Someone interesting to go to a baseball game with. These are things I pay money for. I pay a lot of money to go to games. How much I enjoy it is directly proportional to who I go with. All these things involve connecting people with people. So much money to be made here. Why doesn't the news industry help me meet interesting people?#

Maybe that's why Facebook makes so much money. Just sayin. #

I also am always in the market for better Internet connectivity. Could the NY Times help me there? We all live in the same city. They help me find good restaurants. Maybe if they helped me find better Internet, or if they can't, because it doesn't exist, if they helped to bring us better Internet by constantly beating the drum for it, which is something they can do and seem to like doing -- that would be worth paying for. Beat the drum for new commerce, and then make it possible to buy the thing through your site?#

There are honest ways to make huge money on the Internet. I think the message you're getting from your readers is that advertising is dishonest. The ads you show us net-net are junk. Jokes. Sad. Please stop this. #

Maybe the more distilled message is this: Stop talking so much. Listen. #

The really interesting -discussion- question:

- How much stuff ***should*** there on the Internet?
- How big should the Internet be?
- How many people SHOULD it support?
- Isn't the real problem that the advertising model, the incredible ease with which a site could generate income, has allowed too many sites to exist offering barely worthwhile content?

FireEye Security / September 22nd (today)

- https://www.fireeye.com/blog/threat-research/2015/09/malvertising_attack.html
- From Sept. 8 to Sept. 15, 2015, the Forbes.com website was serving content from a third-party advertising service that had been manipulated to redirect viewers to the Neutrino and Angler exploit kits. We notified Forbes, who worked quickly to correct the issue.
- URLs seen as referrers in the requests:
    - /sabbatical-leave-work-leadership-careers-advice.html
    - /should-the-fda-require-cv-outcome-studies-for-diabetes-drugs-before-approval/
    - /business/the-worlds-100-highest-paid-athletes
    - /investing/the-grateful-graduates-index-2015-the-top-50-roi-colleges/
    - /lists/the-richest-person-in-every-state/
- Redirects browser through a chain of domains
- Javascript running an Adobe Flash file containing SEVEN different exploits.
    - Flash, cve-2015-5119
    - Flash, cve-2015-5122
    - Angler EK's IE cve-2015-2419 exploit
    - IE, cve-2013-2551
    - Flash, cve-2014-0569
    - Vbscript, cve-2014-6332
    - Vbscript, cve-2014-6332
- Conclusion:
    - Malvertising continues to be an attack vector of choice for criminals making use of

exploit kits. By abusing ad platforms – particularly ad platforms that enable Real Time Bidding, which we've covered before here – attackers can selectively target where the malicious content gets displayed.

When these ads are served by mainstream websites, the potential for mass infection increases significantly, leaving users and enterprises at risk.

iOS 9 Content Control App Solutions & Features

Crystal Dean Murphy $1

- No provision for whitelisting
- Report:
- Ads not blocked
- Website broken

Purify Blocker Chris Aljoudi $4

- Super simple whitelisting

Blockr Tim Pollert $1

- Pop-up Whitelist
  - Ad blocker exception
  - Media blocker exception
  - General privacy blocker exception
  - Social button exception
  - Cookie blocker exception

Peace Marco & Ghostery $3

- Overall Config:
- Enable
- Block Social Widgets
- Block External Fonts
- Hide Comments (Discus)
- Add Unrestricted Site
- Pop-up
- Peace Settings
- Same Global Config options + "Bypass for this site"
- Open in Peace
- Open Unrestricted

Silentium Francesco Zerbinati $2

- Optional blocking:
- Images
- Scripts
- Pop-up Whitelisting
- Allow Ads
- Allow Scripts
- Allow Images

1Blocker Salavat Khanov $3 (Free limited)

- TOTALLY configurable
  - 2922 Ad block rules
  - 3993 Tracker blocking rules
  - 7 Twitter widget blocking rules
  - 9 Facebook widget blocking
  - 18 other share widgets
  - 2 custom web fonts
  - 2 Discus comments
  - 14 Adult site blocking

- Online package / rule creator/editor
  - http://my.1blocker.com/
    - 1Blocker Editor

Simplest with whitelisting:	**Purify** ($4, uBlock maintainer, strong block lists.)
Compromise:	**Blockr** ($1, ad, media, privacy, social cookies)
Power User:	**1Blocker** ($3, Total control over every blocking rule.)