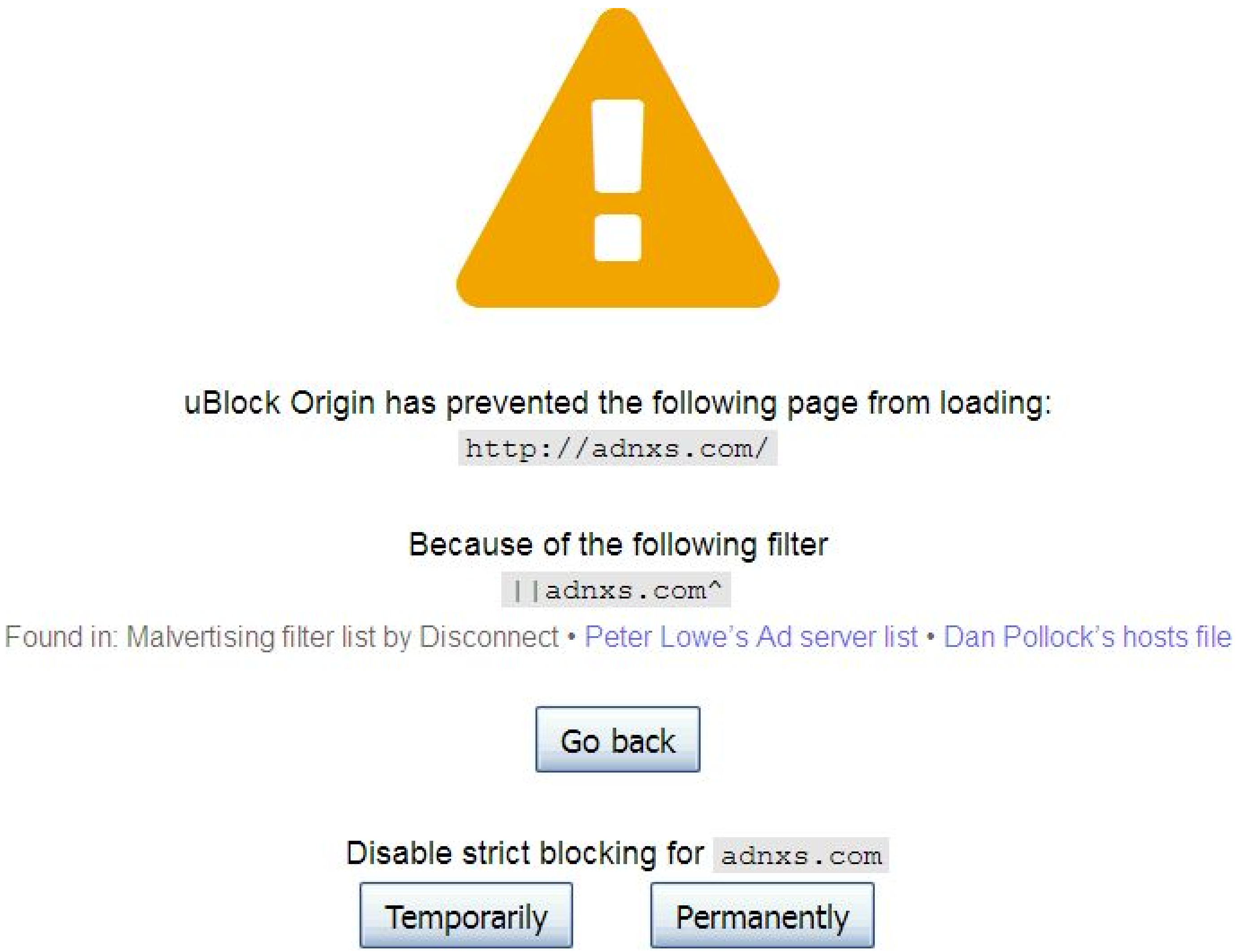
Security Now! #523 - 09-01-15

uBlock Origin

Leo… hearing aid??
Podcast's Audio Quality

This week on Security Now!

- Running Firefox as a "Normal" user
- Malvertising hits MSN
- Amazon & Google tighten up on FLASH
- Windows 7&8 quietly get new and unwanted features
- Dave Winer sounds off
- A bit of miscellany
- uBlock Origin



uBlock Origin has prevented the following page from loading:

`http://adnxs.com/`

Because of the following filter

`||adnxs.com^`

Found in: Malvertising filter list by Disconnect • Peter Lowe's Ad server list • Dan Pollock's hosts file

Disable strict blocking for `adnxs.com`

Security News:

DropMyRights

- Firefox as non-Admin "Normal" user.
    - SAFER_LEVELID_FULLYTRUSTED - Same rights as logged-on user
    - SAFER_LEVELID_NORMALUSER - N : Normal
    - SAFER_LEVELID_CONSTRAINED - C : Constrainted
    - SAFER_LEVELID_UNTRUSTED - U : Untrusted
    - SAFER_LEVELID_DISALLOWED
- ... and anything which is run from Firefox inherits the same reduced rights.

Malvertising: Angler Exploit Kit Strikes on MSN.com via Malvertising Campaign

- https://blog.malwarebytes.org/malvertising-2/2015/08/angler-exploit-kit-strikes-on-msn-com-via-malvertising-campaign/
- "The same ad network – AdSpirit.de – which was recently abused in malicious advertising attacks against a slew of top media sites was caught serving malvertising on MSN.com. This is the work of the same threat actors that were behind the Yahoo! [and Huntington Post] malvertising.

  The incident occurred when people who where simply browsing MSN's news, lifestyle or other portals were served with a malicious advertisement that silently loaded the Angler exploit kit and attempted to infect their computers.

  The ad request came from AppNexus, which loaded the booby-trapped advert from AdSpirit and the subsequent malvertising chain.

  This time, rogue actors are leveraging RedHat's cloud platform, rhcloud.com to perform multiple redirections to the Angler exploit kit (in the previous attack they were using Microsoft's Azure).

  While we did not collect the malware payload associated with this campaign, we believe it is either Ad fraud or ransomware, Angler's trademark.

- Infection Chain:
    - msn.com => lax1.ib.adnxs.com => pub.adspirit.de

- uBlock Origin:
    - adnxs.com - Found in
        - Malvertising filter list by Disconnect
        - Peter Lowe's Ad server list
        - Dan Pollock's hosts file
    - AdSpirit.de: Found in:
        - Malvertising filter list by Disconnect
        - Peter Lowe's Ad server list
        - hpHosts' Ad and tracking servers

Amazon Bans FLASH starting today:

- http://advertising.amazon.com/ad-specs/en/policy/technical-guidelines
  - (Blocked by uBlock Origin due to: "/advertising." in EasyList • Fanboy+Easylist-Merged Ultimate List)
  - Easily allowed by clicking on "Allow Temporarily"

- "Beginning September 1, 2015, Amazon no longer accepts Flash ads on Amazon.com, AAP, and various IAB standard placements across owned and operated domains.
  This is driven by recent browser setting updates from Google Chrome, and existing browser settings from Mozilla Firefox and Apple Safari, that limits Flash content displayed on web pages. This change ensures customers continue to have a positive, consistent experience across Amazon and its affiliates, and that ads displayed across the site function properly for optimal performance.

Chrome Will Begin Pausing Flash Ads By Default, Starting Today (10/1)

- http://techcrunch.com/2015/08/28/chrome-will-begin-pausing-flash-ads-by-default-starting-in-september/
- Google:
  New setting to save power by pausing plugin content
  With today's Beta release of Chrome 42, we've launched a new setting that automatically pauses plugin content that's peripheral to the main page. This can help you save precious battery power and CPU cycles. But don't worry, the primary plugin content on pages (games, videos, etc.) should still run just fine.
- chrome://settings/content
  - Plugins:
  - Run all plugin content (used to be recommended)
  - Detect and run important plugin content
    - (Chrome will automatically run the main plug-in content on websites, but not run peripheral plug-in content.)
  - Let me choose when to run plugin content <-- SMG recommendation.
    - (Chrome will prevent any plug-ins from running automatically, but you can run specific plug-ins by right-clicking on them and choosing "Run this plug-in.")
  - Manage Exceptions

Adam Langley: Intent to deprecate RC4 (this morning)

RC4 is a 28 year old cipher that has done remarkably well, but it is now the subject of several, significant attacks[1][2][3]. The IETF has decided that RC4 is sufficiently bad to warrant a statement that it must no longer be used[4].

When Chrome makes an HTTPS connection it has an implicit duty to do what it can to ensure that the connection is secure. At this point, the use of RC4 in an HTTPS connection is falling below that bar and thus we plan to disable support for RC4 in a future Chrome release. That release is likely to reach the stable channel around January or February 2016. At that time, HTTPS servers that only support RC4 will stop working.

Measurements show that only 0.13% of HTTPS connections made by Chrome users (who have opted into statistics collection) currently use RC4. Even then, affected server operators can very likely simply tweak their configuration to enable a better cipher suite in order to ensure continued operation. (Chrome has long implemented 1/n-1 record splitting and is thus protected against the BEAST attack even with CBC modes and TLS 1.0.)

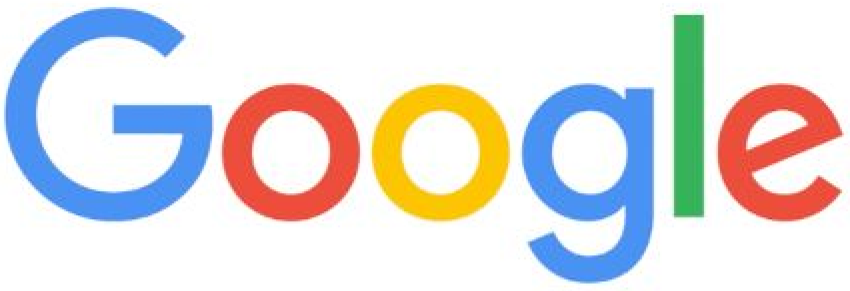
Server operators who don't wish to have to tweak configurations again in the foreseeable future should check that they support TLS 1.2 with ECDHE_RSA_WITH_AES_128_GCM and use the tool at https://ssllabs.com/ssltest to find any other obvious problems.

Current versions of Chrome don't advertise support for RC4 on an HTTPS connection unless the first connection attempt fails, so servers that already support a non-RC4 cipher suite will not see any change.

AGL

Google get a new logo - Biggest update in 16 years!

http://www.fastcodesign.com/3050613/googles-new-logo-is-its-biggest-update-in-16-years



Windows 7&8 Quietly receive user-tracking

- PC-World: Microsoft slips user-tracking tools into Windows 7, 8 amidst Windows 10 privacy storm. Worried about Windows 10's deep-reaching user tracking? Some of it's coming to Windows 7 and 8, too.
    - http://www.pcworld.com/article/2978239/windows/microsoft-slips-user-tracking-tools-into-windows-7-8-amidst-windows-10-privacy-storm.html
- ArsTechnica: "Microsoft accused of adding spy features to Windows 7, 8"
  The privacy impact of Windows' telemetry features continues to be scrutinized.
    - http://arstechnica.com/information-technology/2015/08/microsoft-accused-of-adding-spy-features-to-windows-7-8/

- ExtremeTech: Microsoft backports privacy-invading Windows 10 features to Windows 7, 8
    - http://www.extremetech.com/computing/213183-once-more-with-tracking-microsoft-backports-privacy-invading-windows-10-features-to-windows-7-8
    - FUNNY!
        - Every time Microsoft releases a new version of an operating system, there's always a few users bitterly unhappy at the company's decision not to support new features on older products. Microsoft has finally listened to these die-hard devotees of older operating systems. If you felt like Windows 7 and Windows 8 offered you a little too much privacy, rejoice: Microsoft is updating those operating systems with the same telemetry gathering software it deployed on Windows 10.

          What? You wanted DirectX 12??

- Ghacks: Microsoft intensifies data collection on Windows 7 and 8 systems
    - http://www.ghacks.net/2015/08/28/microsoft-intensifies-data-collection-on-windows-7-and-8-systems/

    - Four recent KB updates for Windows 7/8 designed to send Microsoft regular reports on machine activities.
    - Bypass the HOSTS file:
    - The updates connect to vortex-win.data.microsoft.com and settings-win.data.microsoft.com. These addresses are hard-coded to bypass the hosts file and cannot be prevented from connecting.

- ArsTechnica Summary:
    - As with the other privacy concerns around Windows, our feeling is that the major issue at stake here is not that Windows is collecting data, but that it put the user in control. Collecting information about application errors and the way the operating system is used is reasonable. Having an accurate picture of how people use the operating system is likely to produce a better platform in the future; knowing which applications crash, and why, is obviously invaluable if those apps are to be fixed.

      But we continue to believe that people who do not wish to be a part of such data collection should have a clear and unambiguous way of opting out, and these opt-outs should be rigorous. Disabling CEIP, for example, should not only prevent systems from sending CEIP data, but it should also prevent systems from retrieving even configuration data from Microsoft's own systems. We would also argue that these settings should be made simpler; at the moment there are many individual controls each governing a particular behavior. Some kind of global control to supplement these fine-tuning switches would be an improvement. We like cloud connectivity and online features, but these should be paired with clear user control.

Dave Winer - "Mac OS is spyware too"

- Who is Dave Winer?
  - 60
  - Software developer and editor of the Scripting News weblog.
  - Pioneered the development of weblogs, syndication (RSS), podcasting, outlining, and web content management software.
  - Former contributing editor at Wired Magazine
  - Research fellow at Harvard Law School and NYU
  - Entrepreneur, and investor in web media companies.
  - Received a Master's in Computer Science from the University of Wisconsin,
  - A Bachelor's in Mathematics from Tulane University

- About Him:
  - The Guardian: "When the history of the web is written, his name will be up there in lights, because he was the guy who showed what blogging could do."
  - The New York Times: "The protoblogger."
  - PC World: "The father of modern-day content distribution."
  - Time Magazine: "Helped popularize blogging, podcasting and RSS."
  - The BBC: "The father of blogging and RSS."

- http://scripting.com/2015/08/24/macOsIsSpywareToo.html
- Monday, August 24, 2015 at 8:57 AM
- "Mac OS is spyware too"

  All of a sudden my Mac is telling me whose birthday is tomorrow. People I don't even know that well. How did that happen.

  I don't like my computer randomly and unpredictably getting all "social" on me. It's a tool.

  Try to imagine a carpenter's hammer starting to nag about an upcoming bar mitzvah. A baseball player's bat starting to warn you about overdue bills.
  Who asked for this shit!

Via The Twitter:

- Jeff Price (@jkprice)
  @SGgrc Surprised you liked auto update on Google router. Remote access to router is path to exploit.
- That's a great point, Jeff. But there are many ways for it to be done right. It's the "done wrong" cases that we are always talking about. The router doubtless reaches out to Google periodically to check for anything new, and uses something strong such as certificate pinning and strongly signed firmware, etc. My point is... it's easier to do it wrong, but quite possible to do it right. :)

- NVTweak (@nvtweak)
  - Great stuff... but I'm unable to reply by DM.

Miscellany

- Mr.Robot == Finale tomorrow!

SpinRite

Mike Blommer in Ann Arbor, Michigan
Subject: SpinRite saved my TiVo drive!
:
Hi Steve,
Just wanted to let you know that SpinRite brought my TiVo back to life. My family has been addicted to TiVo for almost 10 years, and I recently turned on my TV to see TiVo stuck on the "Welcome, Powering Up..." message. In searching the various TiVo forums, the most common response is that the hard drive is likely damaged and needs replacing.

I had purchased SpinRite "just in case" last year after becoming a fan of Security Now (and other TWiT podcasts) and I remembered you mentioning that SpinRite will work on TiVo and Linux disks too, so I figured I would give it a try. I hooked-up my TiVo drive to my PC running Windows 8, rebooted into my USB drive configured to run SpinRite, and let it run over night.

There weren't any errors displayed; only "Processed" blocks. But I think I remember you mentioning that SpinRite might still fix the drive even if it doesn't display any errors. So I crossed my fingers that SpinRite fixed the boot part of the drive, and hooked it back up to the TiVo. And voila! The TiVo booted up just fine with all of our recordings!

SpinRite saved me from spending ~$200 on a new TiVo-formatted drive as well as losing many valuable recordings.

Thanks from a relatively newbie listener of Security Now (2 yrs). Love the show! I'm starting to get my 14 yr old son stuck on it (as well as "The Tech Guy"). We don't understand everything (insert picture of deer in the headlights here), but enjoy learning.

---

uBlock Origin

Website Advertising Implied Contract? -- Absolute Nonsense.

- A publicly published website offering opportunistic advertising.
- Roadside billboards:
- Bus: advertisements above the windows.
- Broadcast Television:
- Movie Theaters:
  - Once is was only previews... but now non-movie commercials!
- Advertising-based freeware - 1st spyware - OptOut.
- iTunes ad-supported applications.
  - I will, and do, happily pay to remove ads from an application I actually use.
- Twitter's business model has never been clear, and it shows.
  - If it was necessary to subscribe to post, I would, since I hope I provide valuable links and information to people and I would be glad to keep it up.
  - If it was necessary to subscribe to post, a lot of Twitter's problems would be cleaned up.

- It is not OUR fault is a web site's business model is defective.
    - They publicly display pages at no charge.
    - Those pages contain a mixture of their original content and third-party advertisements.
- Perverse Incentives:
    - More ads = more revenue, but also = more visitor annoyance.
    - As the problem grows an increasing number of visitors will adopt blocking.
- Additional Negatives:
    - Abuse of user's time / bandwidth / battery
    - Abuse of implied trust - tracking
    - Abuse of user's safety - malvertising

The future:

- First-party advertising proxy
- Anti-adblocking -- then the user can determine whether they wish to lower their shields.
    - https://www.playonlinux.com/en/
- (See dark box low-left)
- Logic is similar to what it has always been with NoScript:
    - Surf with Adblocking enabled for speed, sanity, security & privacy
    - IF NECESSARY on a site-by-site basis, weigh the value of dropping blocking.
- Anti-Anti-Adblocking
    - "Anti-Adblock Killer" / Reek on Github / https://github.com/reek/anti-adblock-killer

Raymond Hill == John C. Dvorak x Richard Stallman

- "Gorhill" / Quebec, Canada
- uBlock Origin Background
    - HTTP Switchboard => uMatrix => uBlock
    - 3 months ago, left uBlock, created uBlock Origin
        - Development on uBlock has largely stopped.
    - NO MONEY going to uBlock goes to Raymond.
- All Raymond wants to do is code.

uBlock Origin

- https://github.com/gorhill/uBlock
- Title: "A point-and-click firewall which can be configured on a per-site basis"
- README.md:
    - IMPORTANT: uBlock Origin is NOT an "ad blocker": it is a wide-spectrum blocker -- which happens to be able to function as a mere "ad blocker". The default behavior of uBlock Origin when newly installed is to block ads, trackers and malware sites -- through EasyList, EasyPrivacy, Peter Lowe’s ad/tracking/malware servers, various lists of malware sites, and uBlock Origin's own filter lists.
- Philosophy:
    - uBlock Origin (or uBlock0) is not an ad blocker; it's a general-purpose blocker. uBlock0 blocks ads through its support of the Adblock Plus filter syntax. uBlock0 extends the syntax and is designed to work with custom rules and filters. Furthermore, advanced mode allows uBlock0 to work in default-deny mode, which mode will cause all 3rd-party network requests to be blocked by default, unless allowed by the user.

That said, it's important to note that using a blocker is NOT theft. Don't fall for this creepy idea. The ultimate logical consequence of blocking = theft is the criminalisation of the inalienable right to privacy.

Ads, "unintrusive" or not, are just the visible portions of privacy-invading apparatus entering your browser when you visit most sites nowadays. uBlock0's main goal is to help users neutralize such privacy-invading apparatus — in a way that welcomes those users who don't wish to use more technical, involved means (such as µMatrix).

EasyList, Peter Lowe's Adservers, EasyPrivacy and Malware domains are enabled by default when you install uBlock0. Many more lists are readily available to block trackers, analytics, and more. Hosts files are also supported.

Once you install uBlock0, you may easily un-select any of the pre-selected filter lists if you think uBlock0 blocks too much. For reference, Adblock Plus installs with only EasyList enabled by default.

Features:

- Global and per-site (sticky site-specific) ad blocking
- Curated 3rd-party lists of blocking rulesets
- Uses an enhanced AdBlockPlus (ABP) rule-engine.
- Optional advanced features allow:
    - Extra blocks to be enabled globally or by site
- Individual rules to be

www.wired.com:

- 45.83 seconds / 125 requests
    - 33 of 33 domains connected
- 4.84 seconds / 98 requests
    - 10 of 24 domains connected

Basic Mode:

- https://github.com/gorhill/uBlock/wiki/Quick-guide:-popup-user-interface
- Tooltips enabled
- Click the big POWER icon to sticky-enable/disable uBO for the site.
    - Ctrl-Click for same only for the page.
- Element Picker
    - Interactive object pick & block rule generation.
- Request Log
    - Inspects real-time requests within the browser.
    - Open the request log, hit the "Refresh" button... watch.
- Toggle pop-ups
    - By default, popups *are* allowed unless blocked by a specific filter.
    - Test pop-up blocking:
        - http://jessehakanen.net/adblockpluspopupaddon/test.html
- Toggle strict blocking (for the current site)
    - The 1st-party domain you are attempting to visit is ALSO subjected to filtering.

    - (AdBlockPlus never filters the 1st-party domain, only referred domains.)
    - (This is new behavior as of v9.3.0)
    - Blocks: http://www.sourceforge.net/
- Toggle cosmetic filtering
    - (Number shows how many things were blocked.)
- Toggle remote fonts (due to past font exploits)
    - (Number shows number of 3rd-party fonts used by the page.)

A note about fonts:

- Due to security & privacy concerns, many prefer to block all web fonts by default. This can be done by adding this rule directly in the "My rules" pane in the dashboard:
    - no-remote-fonts: * true
- This will block all web fonts everywhere by default, and they can be enabled on a per-site basis.

Advanced Mode:

- No Tooltips for "Advanced Users" (advanced users are annoyed by them? :/)
- Click the black version bar to open uBlock Settings.
- Check the "Advanced Mode"
- Now (+) appears on the grey bars
- "Static filtering" refers to the filters generated from the various filter lists.
- "Dynamic Filtering" - are firewall rule-like overrides
    - First wide column: What to dynamically handle
    - Object types:
        - "everything" / images / 3rd-party / inline scripts / 1st-party scripts / 3rd-party scripts / 3rd-party frames
    - Domains:
        - All specific 3rd-party domains
    - The left-edge coloration shows whether:
        - Red : all requests were blocked
        - Yellow : some were blocked and some were allowed
        - Green : all requests were allowed
    - Second column:
        - GLOBAL OVERRIDE - everywhere on all sites.

    - Third column:
        - Local override for the current site.
        - The +'s and -'s are log(10) how many requests were allowed or blocked.
            - 1-9, 10-99, >100
            - blank means none blocked

    - Dynamic Rules are TEMPORARY unless you click the padlock.
    - Filtering flow diagram:
        - https://github.com/gorhill/uBlock/wiki/Overview-of-uBlock's-network-filtering-engine

Lowest overhead, Highest performance:

- https://www.raymond.cc/blog/10-ad-blocking-extensions-tested-for-best-performance/view-all/
- 10 Ad Blocking Extensions Tested for Best Performance

Cloud storage (Sync) new in v1.1.0.0

- Uses the native browser's underlying sync'ing feature.
- https://github.com/gorhill/uBlock/wiki/Cloud-storage
- BE SURE TO READ ALL of the preceding page (especially at the bottom!)