

Security Now! #639 - 11-28-17

News & Feedback

This week on Security Now!

This week we discuss a new bad bug found in the majority of SMTP mailing agents, 54 high-end HP printers found to be remotely exploitable, more than 3/4ths of 433,000 websites are using vulnerable JavaScript libraries, horrible free security software, some additional welcome Firefox news, a bit of errata, some fun miscellany, and a BUNCH of feedback from our listeners including reactions to last week's Quad 9 recommendation.

Our Picture of the Week

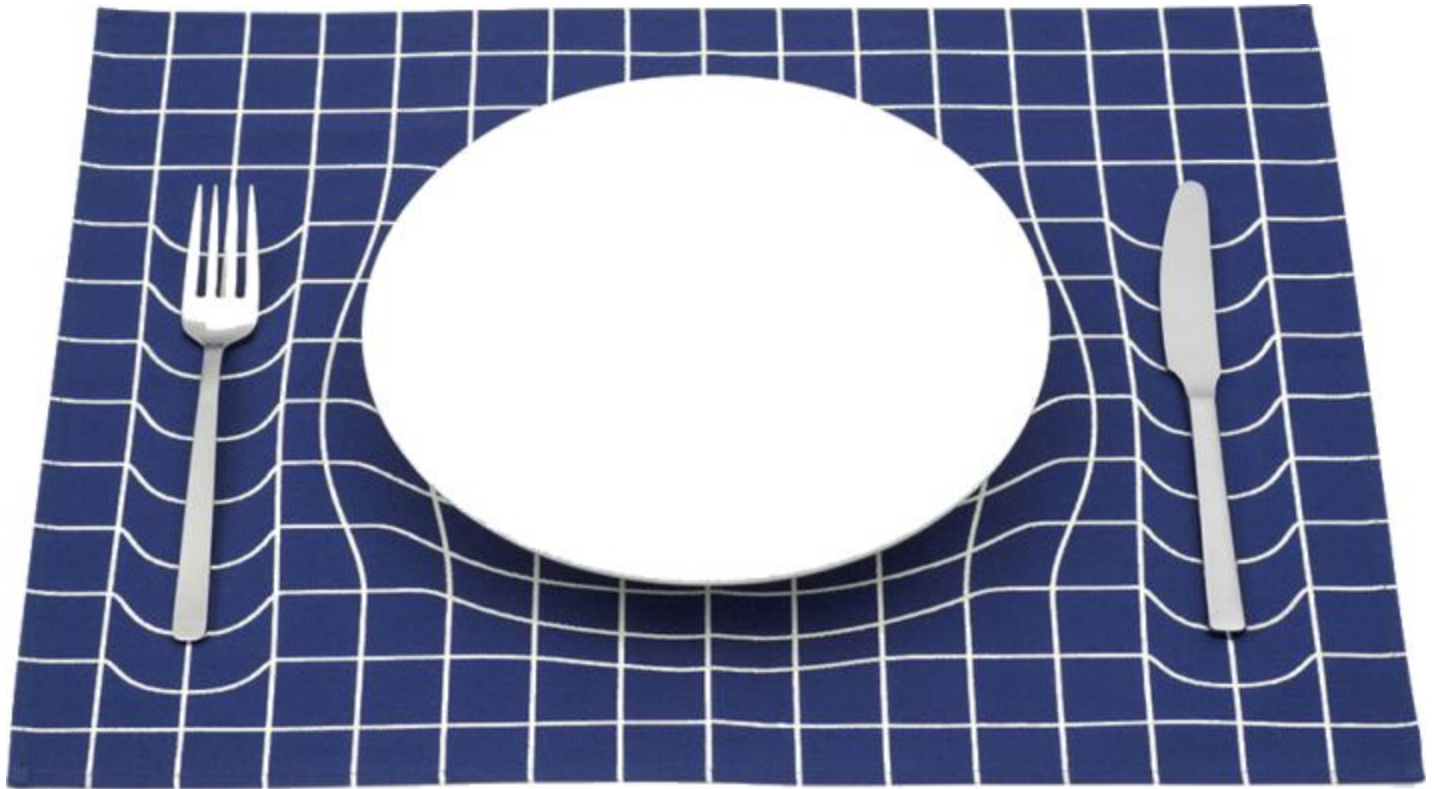
 Comcast 
@comcast

We do not and will not block, throttle, or discriminate against lawful content. We will continue to make sure that our policies are clear and transparent for consumers, and we will not change our commitment to these principles.

 Lore
@loresjoberg

We never will, but it's very important that we be able to. But we won't. So let us do it. Because we won't do it. Which is why we're spending so much money to make sure we can. But we won't. But let us.

The best placemat ever conceived



<https://store.moma.org/kitchen-dining/table-linen-accessories/trick-placemat/125067.html>

Security News

Exim Internet Mailer Found Vulnerable to RCE And DoS Bugs; Patch Now

Exim is an extremely popular mail transfer agent (MTA) used on Unix-like operating systems similar to the venerable Unix Sendmail. It is free software distributed under the terms of the GNU General Public License.

Exim has been ported to most Unix-like systems, as well as to Microsoft Windows using Cygwin and it is the default MTA on Debian GNU/Linux systems.

Many UK-based ISPs and Universities use Exim and it is widely used with the GNU Mailman mailing list manager, and cPanel.

This past March (2017) a study performed by E-Soft, Inc. revealed that approximately 56% of the publicly reachable mail-servers on the Internet ran Exim.

So, against this backdrop, over this past Thanksgiving holiday, a security researcher discovered and publicly disclosed two critical vulnerabilities in Exim, one of which could allow a remote attacker to execute malicious code on the targeted server.

CVE-2017-16943, the first vulnerability, is a use-after-free bug that could be exploited to remotely execute arbitrary code in the SMTP server by crafting a sequence of BDAT commands.

CVE-2017-16944, the second vulnerability, is a denial of service (DoS) flaw that could allow a remote attacker to hang Exim servers and prevent them from accepting and processing SMTP mail connections.

Python-based proof-of-concept (PoC) code has been released, and a Shodan scan reveals that more than 400,000 servers are currently vulnerable.

The vulnerabilities are present in recent Exim versions 4.88 and 4.89, and all sysadmins are recommended to update to Exim version 4.90 which has been released on GitHub.

<https://github.com/Exim/exim>

"Insufficient Solution DLL Signature Validation allows potential execution of arbitrary code."

54 HP Printer Models for Enterprises Remotely Vulnerable to Attackers

The HP printers are running Windows CE.

Recall that many years ago we discussed concerns over the contents of hard drives contained in decommissioned high-end enterprise printers.

The hard drive built into the printer is FIPS-standard encrypted. So the entire contents of the drive is stored in encrypted format, the key for which is provided at boot time. Therefore the researchers were unable to remove the drive to extract its contents.

So... they substituted a standard non-encryption-supporting drive, reinstalled the OS and firmware from a USB thumb drive -- as if recovering from data loss... and they were then able to remove the drive to extract and examine its contents.

<quote> "Both HP Solutions and firmware updates consist of a single file with a ".BDL" (bundle) extension. This is a proprietary binary format with no publicly available documentation. We decided that reverse engineering this file format would be beneficial, as it would allow us to gain insight into exactly what firmware updates and software solutions are composed of."

From Github:

BDL_Patcher

This python script can be used to create modified but still valid HP software solution bundles. Usage instructions are built into the tool. All you need to do is open "mod.zip", replace or add any files that you would like, and then run the following command: python hp_solution_patcher.py orig.bdl orig.zip mod.zip This will generate a new, modified BDL file called patched.bdl

<quote> There exist a number of methods for updating the firmware of HP printers. Most administrators would be aware that firmware updates can be installed through the printer's web interface and through the "Web Jet Admin" client. Firmware can also be installed at boot time through BOOTP/TFTP options. Additionally, the Security settings page on the HP printers implies that firmware can be installed through a print job over port 9100.

Thus... there are a number of avenues available for remote network injection of malicious firmware into HP printers.

Researcher's report:

<https://foxglovesecurity.com/2017/11/20/a-sheep-in-wolfs-clothing-finding-rce-in-hps-printer-fl eet/> Code on Github: <https://github.com/foxglovesec/HPwn>

List of affected printers: HPSBPI03569 rev 1 - HP LaserJet Enterprise printers, HP PageWide Enterprise printers, HP LaserJet Managed printers, HP OfficeJet Enterprise printers, Execution of arbitrary code: <https://support.hp.com/nz-en/document/c05839270>

77% of 433,000 Sites Use Vulnerable JavaScript Libraries

<https://snyk.io/blog/77-percent-of-sites-still-vulnerable/>

It turns out, that if you carry at least one known vulnerability, you likely carry more. 51.8% of vulnerable sites carry more than one known security vulnerability. While the majority of those sites carry one or two, the long-tail is scary. 9.2% of sites carry libraries with a combined four or more known security vulnerabilities.

<i>Library</i>	<i>Detection Count</i>	<i>Adoption %</i>
jQuery	344,643	82.4%
jQuery UI	83,075	19.9%
Modernizr	63,122	15.1%
Bootstrap	57,154	13.7%
Yepnope	41,537	9.9%
FlexSlider	33,002	7.9%
Underscore	17,633	4.2%
Google Maps	14,312	3.4%
Moment.js	14,038	3.4%
SWFObject	13,521	3.2%

Now, let's change it up and look at which libraries are found to be carrying known vulnerabilities. The top couple of names on the list are very similar.

<i>Library</i>	<i>Number of times found vulnerable</i>	<i>% of all instances of this lib detected</i>
jQuery	318,786	92.5%
jQuery UI	74,486	89.7%
Moment.js	10,245	73.0%
AngularJS	7,609	84.8%
Handlebars	3,129	60.7%
Mustache	1,925	51.0%

YUI 3	559	40.3%
jQuery Mobile	413	3.7%
Knockout	407	19.6%
React	181	10.2%

Looking at the percentages doesn't paint a rosy picture. 92.5% of jQuery versions, the most popular library on the web by far, in production carry a known security vulnerability. In fact, of the ten libraries most commonly found to be carrying a known vulnerability, six of them are vulnerable in the majority of versions found in production.

This is the case despite the fact that every one of the libraries on this list has versions available that do not carry these vulnerabilities.

Library	Oldest Version with No Known Vulnerabilities	Release Date
jQuery	3.0.0	June, 2016
jQuery UI	1.10.0	January, 2013
Moment.js	2.15.2	October, 2016
AngularJS	1.6.1	December, 2016
Handlebars	4.0.0	September, 2015
Mustache	2.2.1	December, 2015
YUI 3	3.10.3	June, 2016
jQuery Mobile	1.2.0	October, 2012
Knockout	3.0.0	October, 2013
React	0.14.0	October, 2015

Each of the front-end libraries most commonly found to be vulnerable has been free of known vulnerabilities for anywhere from one to five years. The reality is that front-end libraries and frameworks often don't get updated after they hit production.

Treasury Department Concludes Fraud Investigation into ComputerCOP "Internet Safety" Software

Three years ago, on October 1st, 2014, the EFF posted a detailed takedown of "ComputerCOP" <https://www.eff.org/deeplinks/2014/09/computercop-dangerous-internet-safety-software-hundreds-police-agencies>

For many years it has been purchased in bulk by law enforcement agencies around the US and then freely distributed as a public service and public relations freebie by local agencies to their communities. In one case a sheriff's department bought a copy for every family in its county. At the time of the EFF's article they found it being distributed by 245 agencies in more than 35 states.

So what's the problem? Among its several features is a keystroke logger which records the keyboard activity of all of a computer's users, stored them unencrypted on the system's hard drive, and when it encounters a keyword that might be questionable, eMails the unencrypted stored text, unencrypted, to a central server, where it is then eMailed back to the household's parents.

The software is marketed with invalid endorsements purportedly from the U.S. Department of Treasury, which has issued a fraud alert over the document. And ComputerCOP's publisher claims an apparently nonexistent endorsement by the American Civil Liberties Union and an expired endorsement from the National Center for Missing and Exploited Children. Even IF those endorsements were ever legitimate, they were not backed by any responsible investigation into the design and operation of the product.

That was three years ago.

Today, the EFF is able to report that the U.S. Treasury department has concluded its fraud investigation into this ComputerCOP "Internet Safety" software.

<https://www.eff.org/deeplinks/2017/11/treasury-inspector-general-concludes-fraud-investigation-computercop-internet>

The department did find that the company had forged documents which it had been using as marketing material for its products, and that those forged documents were instrumental in the sales of the software to law enforcement agencies.

However, the 3-year statute of limitations had since expired, and the forged documents were no longer present on the company's website or marketing materials.

The software DOES, however, continue to be sold and offered free of charge to the public where the software is promoted as a "Perfect Election and Fundraising Tool!" In the EFF's follow-up report they wrote: In 2017 the Lake County Sheriff's Office in Florida purchased 1,000 copies for \$5,975 according to SmartProcure. And McGruff the Crime Dog was handing out copies this summer at a community screening of the film "Elf" in Islip, New York.

The takeaway for our listeners -- and anyone they know -- is to stay as far away from this "ComputerCOP" spyware as possible.

Firefox plans to flag sites that have been hacked in the past

<https://www.bleepingcomputer.com/news/security/firefox-will-warn-users-when-visiting-sites-that-suffered-a-data-breach/>

Mozilla's Firefox will be teaming up with Troy Hunt's "Have I Been Pwned" database.

"Have I Been Pwned" currently maintains a growing list of 254 websites that have had their user's password databases exfiltrated in the past. The new feature planned for Firefox will check any sites its users visit and preemptively warn them when they are visiting any site that has, in the past, suffered a breach of their user's secret data.

Firefox won't block or prevent the visit, but it will raise a caution about the site's past security.

Naturally, breached websites won't like this, but users will... and it is hoped that the spectre of keeping past breaches more current may serve to keep companies more focused upon not being added to that list in the future.

Errata

- Fixed the "Oct" should be "Nov" typos on the SN page. Thanks all!!
- chy / @jchybow
@SGgrc correction about the role of USCentCom Steve, it's not inherently an "intel gathering op." It's a theater-level combatant command (under which there are many, many sections).

Miscellany

Two Humble Bundles

- Java
<https://www.humblebundle.com/books/java-books>
SIX days remaining
- Science Fiction
<https://www.humblebundle.com/books/scifi-fantasy-tachyon-books>
EIGHT days remaining

Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa

<https://powercompare.co.uk/bitcoin/>

- In the past month alone, Bitcoin mining electricity consumption is estimated to have increased by **29.98%**
- If it keeps increasing at this rate, Bitcoin mining will **consume all the world's electricity by February 2020.**
- Estimated annualised global mining revenues: **\$7.2 billion USD (£5.4 billion)**
- Estimated global mining costs: **\$1.5 billion USD (£1.1 billion)**
- Number of Americans who could be powered by bitcoin mining: **2.4 million** (more than the population of Houston)
- Number of Britons who could be powered by bitcoin mining: **6.1 million** (more than the population of Birmingham, Leeds, Sheffield, Manchester, Bradford, Liverpool, Bristol, Croydon, Coventry, Leicester & Nottingham combined) Or Scotland, Wales or Northern Ireland.
- Bitcoin Mining consumes more electricity than **12 US states** (Alaska, Hawaii, Idaho, Maine, Montana, New Hampshire, New Mexico, North Dakota, Rhode Island, South Dakota, Vermont and Wyoming)

SpinRite

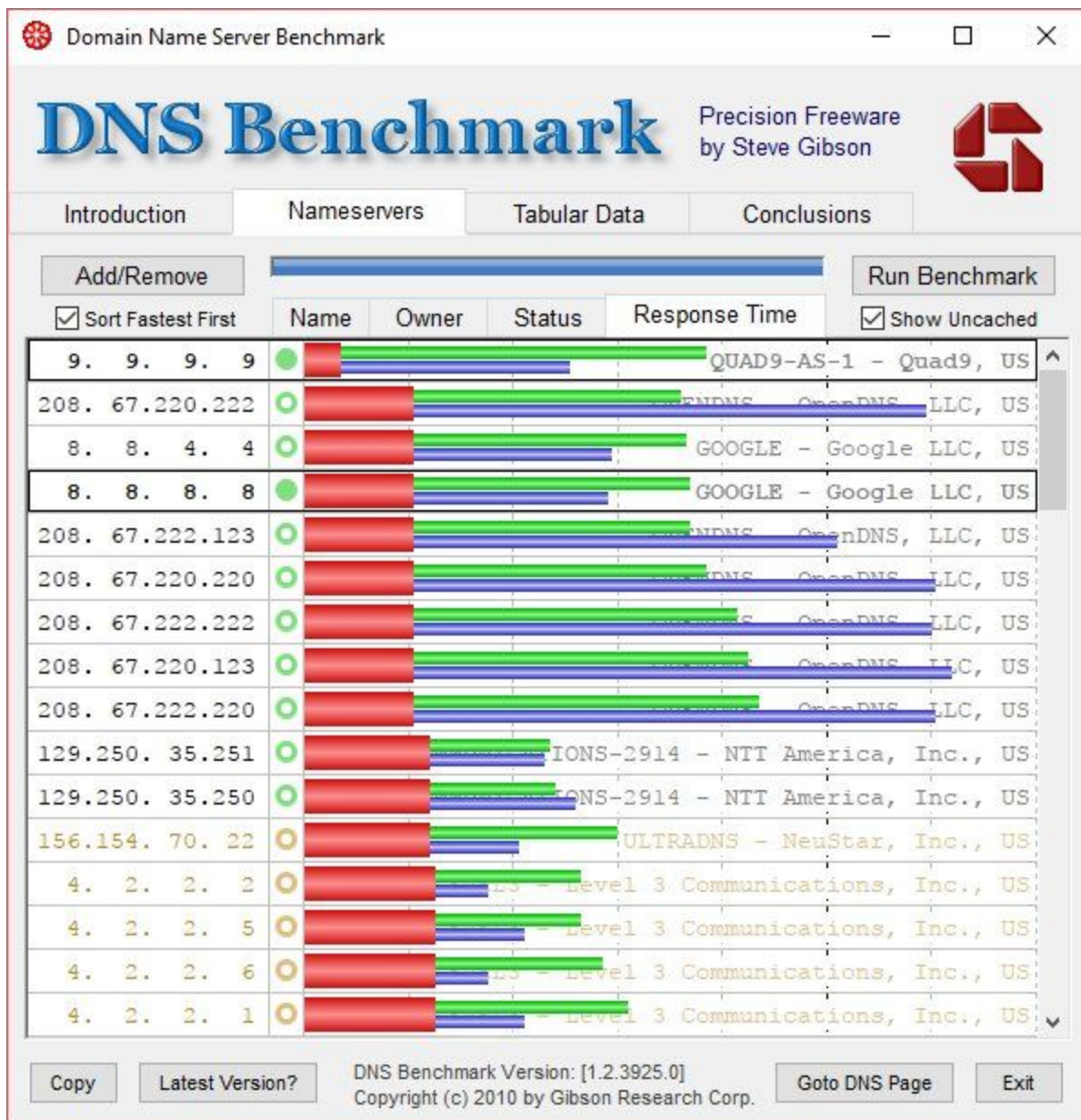
Chad Emory / @lab_doc

@padresj @SGgrc I keep hearing of people using SPINRITE on Android phones, standard build and MS boot build will not see phone on USB. Is there a trick on how to get it to work with Samsung phones?

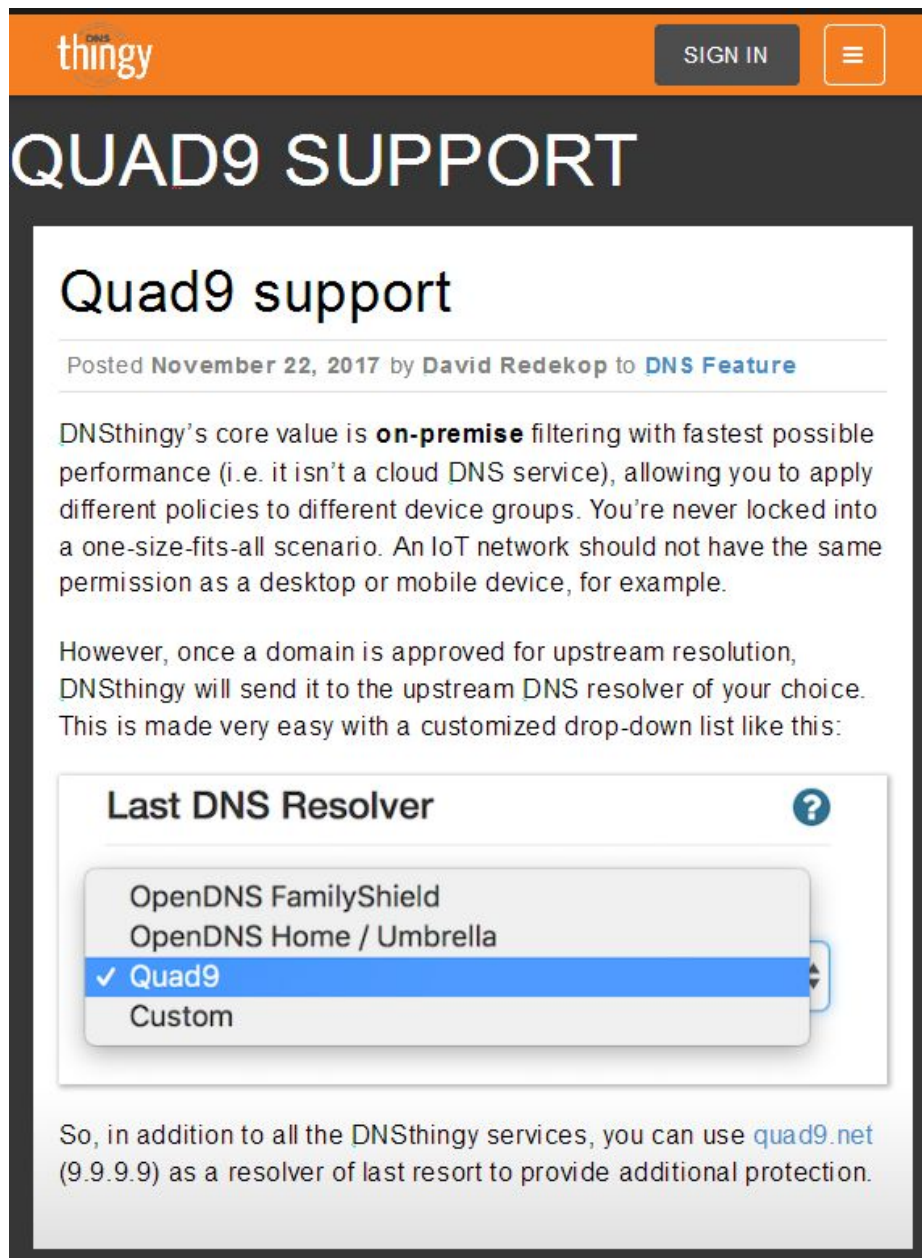
Closing The Loop

Quad Nine Follow-ups:

- **Jason Egan / @beguil3d**
Hey @SGgrc - with respect to #Quad9 - do you suggest we utilize any secondary DNS (Google's 8.8.8.8 for instance) or use 9.9.9.9 solely? I'm giving Quad9 a go on my network now and was curious. Thanks!
- **Dan Kutka / @dkutka25**
@SGgrc switched over to quad9 dns and definitely see better performance than open dns and safe dns I was using previously. a nice addition to my tool kit.
- **Kevin Sanders / @AZKevin**
I'm taking it to the 9s! Even in Rural Utah #Quad9 is kicking it in gear!



- **Tim Grissom / @tggrissom**
Replying to @SGgrc
In Orland 9999 is slower by x2 than open dns
- **Chris Erice @ChrisErice**
Replying to @SGgrc
Unfortunately, #Quad9 routes Seattle users to Palo Alto, CA (verified via trace route).
Sticking with @opendns for now.
- **Justin Alcorn / @JaBbA64**
@SGgrc 9.9.9.10 is for research..so you know if NXDOMAIN is for blacklist reasons
- **David Redekop / @DRtheNerd**
@SGgrc great Quad9 coverage... just in case you're wondering, yes of course we have
DNSthingy support for it already: <https://www.dnsthingy.com/2017/11/quad9-support/>



The image is a screenshot of a web page from DNSthingy. At the top, there is an orange navigation bar with the 'thingy' logo on the left, a 'SIGN IN' button in the center, and a hamburger menu icon on the right. Below the navigation bar, the main heading 'QUAD9 SUPPORT' is displayed in large, white, bold letters against a dark background. The article content is on a white background. The title 'Quad9 support' is followed by a sub-header 'Posted November 22, 2017 by David Redekop to DNS Feature'. The main text explains that DNSthingy's core value is on-premise filtering with fast performance, allowing for different policies for different device groups. It then states that once a domain is approved for upstream resolution, DNSthingy will send it to the upstream DNS resolver of choice, which is made easy with a customized drop-down list. This list is shown in a screenshot of a web interface titled 'Last DNS Resolver' with a help icon. The list includes 'OpenDNS FamilyShield', 'OpenDNS Home / Umbrella', '✓ Quad9' (which is highlighted in blue), and 'Custom'. Below the screenshot, the text concludes that in addition to all DNSthingy services, users can use quad9.net (9.9.9.9) as a resolver of last resort for additional protection.

Dave Hay / @david_hay

@SGgrc Hey Steve, have you yet had a chance to test Firefox Quantum and LastPass ? If so, what's your verdict thus far ? Thanks, Dave

Moriturimax / @moriturimax @SGgrc about the Amazon Key freezing camera, couldn't you just put a big fan or other moving object (blinking LEDs) in view of the camera to tell if it's frozen or active? Perhaps even a string of blinking Christmas lights?

Andrew / @ISpaceCab

@SGgrc on security, could you make a comparison between Telegram & Signal messaging apps?

Yes: Telegram is closed source using a very bizarre, home-grown, untested and unknown encryption protocol. Signal is open source, using well-tested, industry standard, encryption with completely documented and very clear additional features added.

Simon Zerafa / @SimonZerafa

@SGgrc Any thoughts in the Intel JTAG bug being deliberate? How useful would such a working attack be on any Intel platform to a Three Letter Agency? ????

Adam van Kuik / @avankuik

@SGgrc What was the 19 book series you were talking about earlier this year? You mentioned it a few times on Security now and I believe you said you read it twice.

Ove Karlsson / @KarlssonOve

Thank you @SGgrc, got bored on friday, went scrolling through Netflix and The Expanse was on one of the cards. Remembering you raving about it on SN, so I gave it a go, now a 2 day and 2 season binch later I can't wait for season 3. #TheExpanse #SN #GreatTip #ThankYou

John Arundel @bitfield

Mind. Blown. "Pingfs is a filesystem that stores data in the Internet itself, as ICMP packets going to remote servers and back" github.com/yarrick/pingfs
(Several years old... but a fun idea reminiscent of mercury delay lines.)

jmwhitty / @jmwhitty

@SGgrc @leolaporte when you talk about Apple vs FBI re: golden keys, you often do not mention the impact to the non Apple's of the world

Michael Synan / @mike_synan

@SGgrc any suggestion for network firewall hardware not containing IME? Or how to build an uncompromised network firewall without the hardware hack discussed two episodes ago?

Kyle / @craigconsulting : @SGgrc @leolaporte Hey Steve if you think watching disc defragmentation is mesmerizing, you should try watching a 3D printer at work! #soothing

Will Springer / @W_L_Springer : @SGgrc On Security Now, you and Leo were discussing the trend and importance of "pushing" updates to IoT devices to patch firmware vulnerabilities. Would that functionality create a new vector for a party to push malicious firmware to these devices? Thank you!