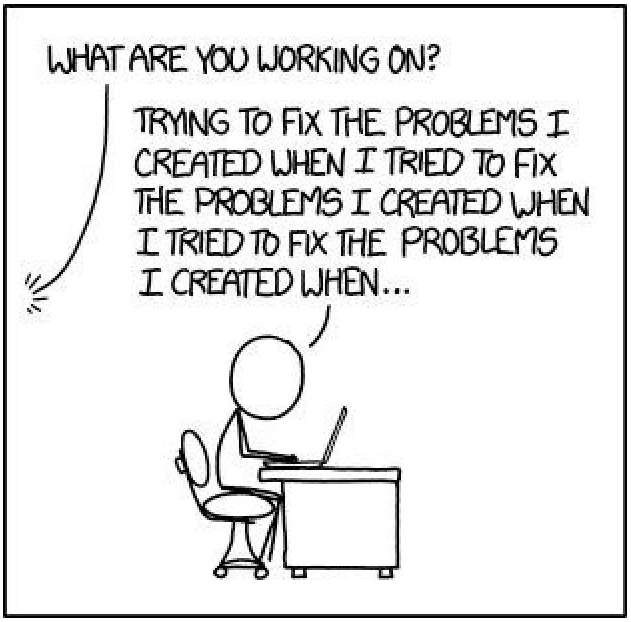
Security Now! #580 - 10-04-16
Q&A #240

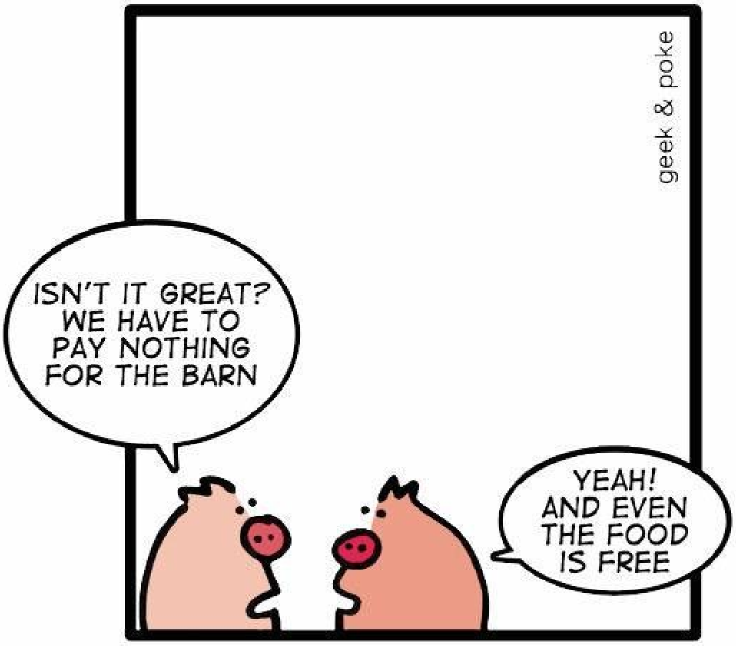
This week on Security Now!

- An "update" on Microsoft's GWX remover,
- An encouraging direction for the Windows 10 Edge browser,
- HP in the doghouse,
- "Oh yeah, that's what I meant to say about how to upgrade a site's password hashing",
- A really terrific Dynamic DNS hack,
- Another update on Windows update,
- A distressing heads-up about how some unseen behavior of our web browsers is fatiguing our SSD's,
- A bit of errata, miscellany, and then a discussion of feedback from our terrific listeners.

The Challenging of fixing complex things


WHAT ARE YOU WORKING ON?
TRYING TO FIX THE PROBLEMS I CREATED WHEN I TRIED TO FIX THE PROBLEMS I CREATED WHEN I TRIED TO FIX THE PROBLEMS I CREATED WHEN...

Facebook's WhatsApp is Free!! What a bargain!


geek & poke
ISN'T IT GREAT? WE HAVE TO PAY NOTHING FOR THE BARN
YEAH! AND EVEN THE FOOD IS FREE

Security News

KB3184143 *is* an "Optional" Update.

- So... NOT selected by default, but can be chosen.

Microsoft moving Win10's Edge browser into its own VM

- http://arstechnica.co.uk/information-technology/2016/09/windows-10-will-soon-run-edge-in-a-virtual-machine-to-keep-you-safe/
- Microsoft has announced that the next major update to Windows 10 will run its Edge browser in a lightweight virtual machine to make exploiting the browser to attack the underlying operating system, or compromising user data, significantly more challenging.
- This new isolation will be called: Windows Defender Application Guard for Microsoft Edge.
- Edge is already running in a constrained Sandbox
- Putting Edge into a more formal VM further strengthens the browser's isolation.
- BUT!! ---> ONLY available on the Enterprise edition of Windows 10.

HP issued an InkJet printer "firmware security update" which blocked non-HP Ink cartridges.
https://www.eff.org/deeplinks/2016/09/what-hp-must-do-make-amends-its-self-destructing-printers

Dion Weisler
President and CEO
HP Inc.
1501 Page Mill Road
Palo Alto, CA 94304
September 26, 2016

Dear Mr. Weisler,

I write to you today on behalf of the Electronic Frontier Foundation, a nonprofit devoted to defending technological freedom, human rights and privacy in courtrooms, legislatures, and online. Like many others, we are alarmed by reports that HP has activated a dormant feature in Officejet Pro printers (and possibly other models), so that the printers now automatically verify whether its ink cartridges are official HP ink and not competitors' products or even refilled HP cartridges. If these printers detect third-party ink, printing stops. This activation was disguised as a security update.

You must be aware that this decision has shocked and angered your customers. Below, I have set out our concerns and the steps HP must take to begin to repair the damage it has done to its reputation and the public's trust.

- HP deprived its customers of a useful, legitimate feature
- HP abused its security update mechanism to trick its customers
- HP's time-delayed anti-feature is a bait-and-switch

https://www.eff.org/deeplinks/2016/09/dont-hide-drm-security-update

EFF: Over 10,000 of you have joined EFF in calling on HP to make amends for its self-destructing printers in the past few days. Looks like we got the company's attention: today, HP posted a response on its blog. Apparently recognizing that its customers are more likely to see an update that limits interoperability as a bug than as a feature, HP says that it will issue an optional firmware update rolling back the changes that it had made. We're very glad to see HP making this step.

Migrating to a more secure password hashing algorithm...

- A number of listeners wondered whether they were missing something, since I had previously described the obviously correct approach to upgrading from a weak password... <g>

A terrific DNS hack!

- Angelo vd Sijpt (@_angelos)
- @hover does not have dynamic DNS, but you can always add a CNAME that points {something.at-hover.com} to {random.afraid.org}
- A CNAME (canonical) is an "alias" for the pointed-to DNS record.
- (CNAMES always point to another DNS name.)
- My two blogs were implemented with CNAMES:
  - steve.grc.com => agilesynapse.wordpress.com.
  - blog.grc.com => grcblog.wordpress.com.

The "Windows 7 Update solution" (Microsoft / Community)

On GRC's LinkFarm page:
http://answers.microsoft.com/en-us/windows/forum/windows_7-update/windows-7-update-solution/f39a65fa-9d10-42e7-9bc0-7f5096b36d0c

> September 13, 2016
>
> Windows Update has become quite problematic for Windows 7 users. For the past year or so, we've been working to find a solution that will work for you. We have found one that works very well indeed for most. We know for certain this works well for September 2nd Tuesday, known as Patch Tuesday. Which is today, and onwards till October 7th.
>
> You want to ensure you get all your Windows Updating done before the next Patch Tuesday, October, 8. From that point onwards, there will be a very significant change in the way Windows Update works. Some may like it a lot. Some may dislike it intensely.

Firefox's Continuous Session Save is Chewing up SSD's
https://www.servethehome.com/firefox-is-eating-your-ssd-here-is-how-to-fix-it/

<Paraphrasing> Firefox users running on SSD mass storage should consider this must-change setting: Today's modern multi-core processor systems and higher quantities of RAM allow users to open multiple Firefox tabs and windows simultaneously. This can have an unintended effect for those SSDs, as session store data is being written constantly to NAND -- thus fatiguing it.

Purely by chance, the author of this report fired up a free copy of SSDLife on two consecutive days on a workstation used only for email and browsing. For those unfamiliar with this tool, it reports estimated lifetime for an attached SSD and it also shows the amount of data read and written.

In this case, SSDLife notified the user hat 12GB was written to the SSD in one day. Since he didn't recall downloading any huge files over the previous day or visiting any new sites that could've resulted in bringing down a lot of new content to the cache, this puzzled him. He monitored these stats over the next couple of weeks and this behavior stayed consistent. Even if the workstation was left idle with nothing running on it but a few browser windows, it would invariably write at least 10GB per day to the SSD.

Using SysInternals Resource Monitor's disk utilization immediately revealed the culprit: FireFox. It was writing continuously between 300K and 2MB per second to a file named "recovery.js." This is FireFox's session backup file which is used to restore browser sessions in case of a browser or an OS crash or hang.

(See the article for full details.)

about:config
browser.sessionstore.interval / default 15000 (mS) - so every 15 seconds.

It is set to 15 seconds by default. This experimenter set it to a more sane (at least for him) 30 minutes. Since then, he's only seeing about 2GB written to disk when his workstation is idle, which still feels like a lot but is 5 times less than before.

Bottom line is that if you have a lower capacity consumer level SSDs in some of your machines, you may want to check and tweak your Firefox config. Those drives can be rated for about 20GB of writes per day and Firefox alone might be using more than half of that. This is especially true if you're like him and have a several browser windows open at all times each with numerous tabs. Changing this parameter may even help with normal HDDs. Your machine will feel faster if it doesn't have to constantly write this session info. Users have observed that content open in the browser does have a major impact on writes, as does the number of open windows and tabs. If you are using Firefox and a lower write endurance SSD you should check this immediately.

In an update:
Update 1: We are testing other browsers. Currently in the middle of a Chrome Version 52.0.2743.116 m test. We have been able to see a pace of over 24GB/ day of writes on this machine. (1 GB/hour)

Errata

- Jeff Garretson (@jfgrtsn)
  @SGgrc "Corpora."
- (JKL: “corpora”... because third declension neuter.)

Miscellany

HSF - iHerb & Swanson Vitamins are both back in stock.

- At the start of November I'll solicit feedback, results, dosages, etc.

Maciej Targoni's two puzzle toys (Hook and Klocki) are now both free

- https://itunes.apple.com/us/app/hook/id956794130
- https://itunes.apple.com/us/app/klocki/id1105390093

HBO's "WestWorld"

- Premieres October 2nd
- 100% Rotten Tomatoes / 7.4/1O @ tv.com
- Deadline / Hollywood: "‘Westworld’ Review: HBO’s Violent Epic More ‘Grand Theft Auto’ Than ‘Game Of Thrones’"
  <quote> Underneath all its skin-level notions of free will, the open conceit of Westworld is that it is like the open sandbox of multiple storylines and resets found in the hugely successful Grand Theft Auto video game franchise — it can be or do whatever it wants. From what I’ve seen, once the setup of the hour-plus pilot establishes the parameters (or lack there of), that’s what its developers, Jonathan Nolan and Lisa Joy, want to reach for – and what they grab hold of.

SpinRite

Q&A:

[1] - AspiringLockpicker (@AspiringLockpic)

@SGgrc How can I use DNSSEC on windows 10? Your spoof test says my system's servers have DNSSEC. How do I make use of it?

(((Notes))): In Windows 7 and later operating systems, the Windows DNS client is security-aware, which means it can determine whether a DNS response that it receives was validated as genuine or not. The DNS client itself is non-validating, and it depends on a DNS server to provide DNSSEC validation. The client can require that this validation is performed if rules are configured in the Name Resolution Policy Table (NRPT) and applied by Group Policy.
NRPT: https://technet.microsoft.com/en-us/library/dn593632(v=ws.11).aspx

[2] - Wildkarde (@wildkardeuk)

@SGgrc What's the difference between HTTPS and HSTS? And what are the pros/cons/differences? Just finished watching Security Now. Thanks.

[3] - Ian Anderson Gray

Hi Steve. I wrote an article on how to broadcast to Facebook Live from your desktop - iag.me/socialmedia/br? - it's become very popular with over 600 comments. Most people are able to connect without any issues, but it seems that some people can't. I have a feeling some people's ISPs are blocking the connection. Facebook Live uses RTMP and I think this is port 1935. In order to help less techie people, what's the easiest way to check if their ISP is blocking port 1935 and what can they do to get their ISP to unblock it? Could their be another issue? Thanks so much for your time and Security Now - I never miss it! Ian

-----

(((Notes))): RTMP is carried over TCP. (There is a less common UDP version).
GRC utils: ID Serve / ShieldsUP!

[4] - Stijn Crevits

Hey Steve Good news: cPanel does support LetsEncrypt now. But they need to fix a bug where only admins can configure it. One issue with LE's auto-renewal, however, is that you can't use HPKP.

(((Notes))): HPKP supported by Firefox & Chrome, but not IE/Edge.

- cPanel Blog: https://blog.cpanel.com/announcing-cpanel-whms-official-lets-encrypt-with-autossl-plugin/

- HPKP is somewhat like HSTS, it allows a server to provide hashes of its certificates in query response headers, which browser then cache for future comparison
    - https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning

[5] - Chris A

Steve, love Security Now and SpinRite. I would love to follow your advice and offer TLS on my personal website but there's a problem. Let's Encrypt is hosted by the Akamai CDN and I trust Akamai about as far as I can throw a data center. (More on that if you wish.) The much lauded Digicert doesn't appear to have joined the free cert party yet and other free cert issuers have had numerous problems as you've recently detailed on the podcast. Is there a free cert issuer other than Let's Encrypt that you could recommend? Thank you for all you do.

[6] - Ben Moore

Steve, thank you so much for all you do. In 2015 I experienced a compromise of my eBay account. Turns out, eBay has a "feature" where you can have a password reset code sent tot your mobile phone by text message and within the dialog box you can select "Try a different number" if you no longer have access to the phone number associated with your account. After the compromise, I got everything sorted out however now in 2016 - my account was compromised again!!! Oddly enough, by the same phone number as last year. So, after resetting all my passwords (easy enough) I discovered that somehow the phone number used to reset the password is still associated with my account but cannot be corrected/deleted. After a few very long calls to support to correct, the final one ending in me demanding a return call with a resolution (still waiting after a month for a call back) the phone number is still associated with my account. Here's why I'm writing: have you in your experience found a way to correct this sort of problem? Is my account, which has been open since 2001, to be forfeited? Can I better protect myself? I'm hoping your experience can assist, or your exposure might be able to highlight the absolute failure on the part of eBay to be "able" to alter account information for security purposes or frankly willingness to help keep customer accounts secure.