Security Now! #543 - 01-19-16

LostPass

This week on Security Now!

- Major Internet of Things news: Ring Doorbell, Webcams, WiFi Passwords in the Cloud.
- More Malvertising in the news
- Another worrisome major Internet appliance backdoor discovered
- New York State Assembly Bill about Phone encryption
- More Microsoft and Windows 10 news
- A few bits of Errata, Miscellany, a question about long term data archiving
- And... The ShmooCon presentation of the LastPass phishing hack.

Security News:

Ring Doorbell

- Steal your Wi-Fi key from your doorbell? IoT WTF!
  - https://www.pentestpartners.com/blog/steal-your-wi-fi-key-from-your-doorbell-iot-wtf/
  - Starts off sounding like an advertisement for the Ring Doorbell:
    <quote> The Ring is a Wi-Fi doorbell that connects to your home Wi-Fi. It's a really cool device that allows you to answer callers from your mobile phone, even when you're not home.
    It's one of the few IoT devices we've looked at that we might even use ourselves. It acts as a CCTV camera, automatically activating if people come close to your home. You can talk to them, to delivery couriers, to visitors etc. It can even hook up to some smart door locks, so you can let guests in to your home.
    It is genuinely useful! Unlike most IoT devices :-)

  - Until it was (immediately) patched, an installed doorbell could be opened with a Torx T4 driver, the orange "setup" button pressed to bring up a configuration access point, and the device's configured WiFi password could be obtained from an XML file obtained at: URL /gainspan/system/config/network

  - <quote> This is quite a fail: walk up to door, remove doorbell, retrieve users Wi-Fi key, own their network!
    Did Ring ever intend to expose this functionality, or was is this just default functionality that Gainspan have in their firmware? As it's a standard Gainspan URL it looks like they just hadn't disabled the configuration.
    The Wi-Fi key is still stored in the doorbell somewhere - how well protected is it now? It's most likely stored in the module, somebody with a soldering iron could possibly get it.

Having physical access to the doorbell means we might be able to upload modified firmware. Your doorbell becomes a back door?

- HOWEVER
  Kudos is due to Ring for responding to our vulnerability alert within a matter of minutes. A firmware update was released earlier this week that fixes this issue, just two weeks after we disclosed it to them privately. Good job Ring!

- **Ring Responds:**
  100% Of Active Ring Video Doorbells Keep Your Wi-Fi Password Secure
- http://blog.ring.com/index.php/2016/01/13/100-of-active-ring-video-doorbells-keep-your-wi-fi-password-secure/

- Ring Community,

  You may have seen a report that Ring customers' Wi-Fi passwords are currently vulnerable. This is false.

  We became aware of a potential security issue regarding Wi-Fi passwords last year and promptly developed a solution to ensure Wi-Fi passwords are secure with all Ring Video Doorbells. This fix was automatically pushed to all active Ring devices via a firmware update within 24 hours of us releasing the update (no user action required).

  This means 100% of active Ring Video Doorbells are currently operating on a secure version of our firmware and your Wi-Fi password is secure.

  Every day, your Ring device automatically checks for new firmware updates. There is a chance that some Ring devices currently on store shelves have firmware that does not contain the fix. As soon as those devices are set up, the firmware will automatically update to latest version 1.6.39 and there will be no Wi-Fi vulnerability.

  If you'd like to double check that your Ring is operating on the most up-to-date firmware – version 1.6.39 – you can simply open your app, click on your Ring device and go to its "Settings" page to view the version of firmware your device is running (see screenshots below).

  We at Ring work every day to keep your home, neighborhood and community safe. If you have any concerns or would like to speak with a Ring representative for more information about this topic, we're available. Please send an email to security@ring.com and we'll respond promptly.

  Sincerely,
  Joshua Roth
  Chief Technology Officer

- SMG: Repeat after me... *"All of our IoT devices need their own isolated WiFi network."*

Turning a webcam into a backdoor

- Vectra Threat Labs
  http://blog.vectranetworks.com/blog/turning-a-webcam-into-a-backdoor
  Reports of successful hacks against Internet of Things (IoT) devices have been on the rise. Most of these efforts have involved demonstrating how to gain access to such a device or to break through its security barrier. Most of these attacks are considered relatively inconsequential because the devices themselves contain no real data of value (such as credit card numbers or PII). The devices in question generally don't provide much value to a botnet owner as they tend to have access to lots bandwidth, but have very little in terms of CPU and RAM.

  However these devices get more interesting to sophisticated attackers when they can be used to establish a persistent point of access in a network. Putting a callback backdoor into a webcam, for example, gives a hacker full-time access to the network without having to rely on infecting a laptop, workstation or a server, all of which are usually under high scrutiny and may often be patched. On a tiny device, there is no anti-virus and no endpoint protection. In fact, no one thinks of the device as having software on it at all. This makes these devices potentially inviting for persistent attackers who rely on stealthy channels of command-and-control to manage their attacks.

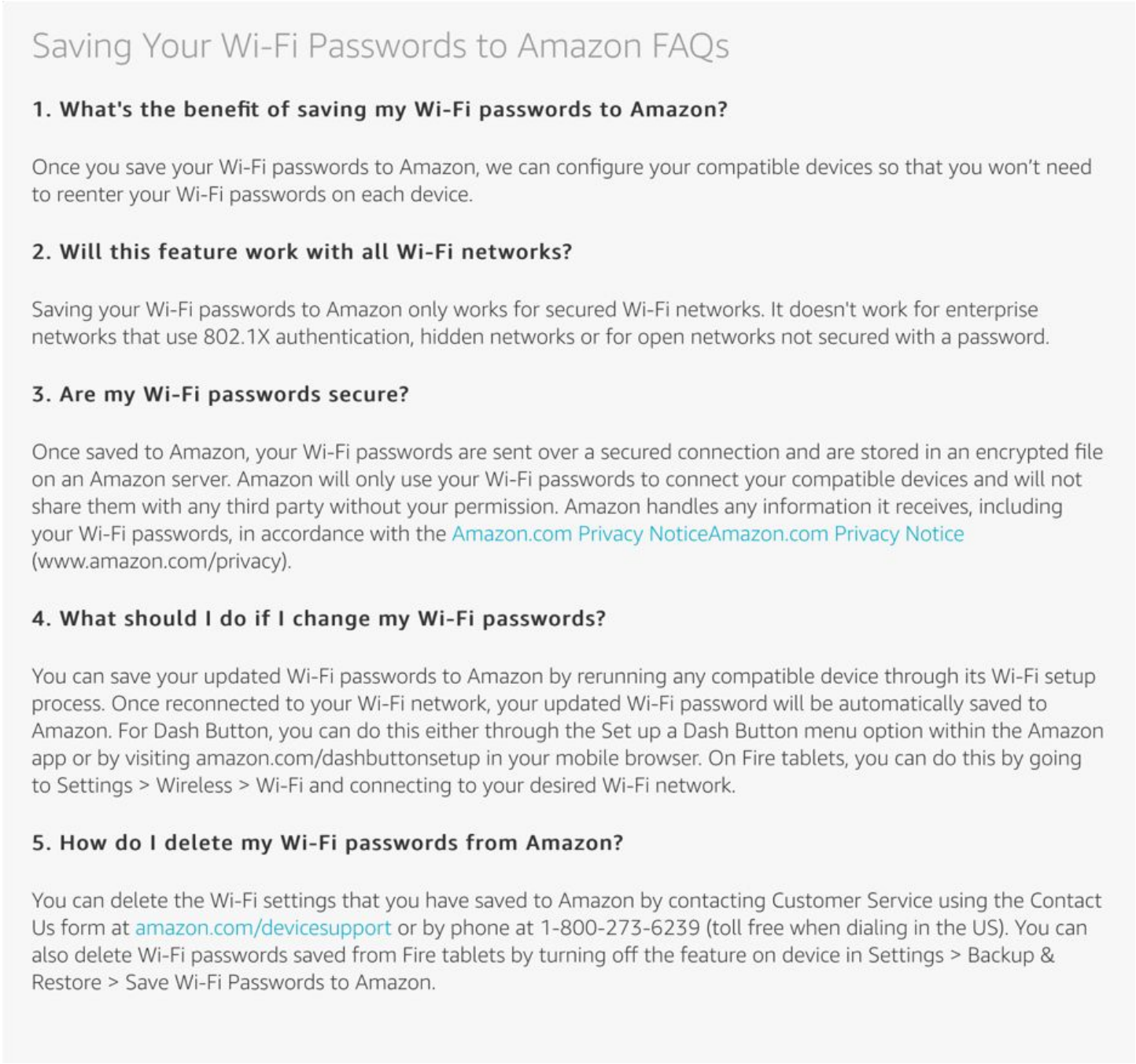
  The downside for the attacker is that this class of devices doesn't usually have any persistent storage that is really usable. Instead, they use nvram to store configuration and the flash ROM to store the running code. So the attacker's hope for real persistence rests on being able to control what will be in the flash ROM. In this blog, we will explore how difficult it is to create a new flash image that could contain all the tools we need to have a real persistent backdoor to the network on which the device is installed. Once we have such a flash image, putting it in place could involve "updating" an already deployed device or installing the backdoor onto the device somewhere in the delivery chain - i.e. before it is received and installed by the end customer. For this experiment to be meaningful, it is imperative that the device continue to perform its normal function otherwise it would immediately raise suspicion or cause the customer to replace the device with a working version.

- **Kaspersky Labs:** The report explains the attack against a $30 D-Link WiFi Webcam, starting with the researchers being able to dump the contents of the device's flash memory chip for analysis. This particular device's firmware included a u-boot and Linux kernel and image. They were also able to dump the contents of the Linux image and access its filesystem, where they found an executable file used to verify and update the firmware. By analyzing the process by which the firmware is updated, they were able to remotely add a connect-back Socks proxy to the Linux system.

- **<quoting from the Vectra report>** "This can either be accomplished with an srelay and netcat in the startup script or more optimized C code, or one could go with a simple callback backdoor with a shell using netcat and busybox which are already present on the system. Using the telnetd / busybox / netcat we can bring back a telnet socket to an outside host to have remote persistence to the webcam. With the webcam acting as a proxy, the attacker can now send control traffic into the network to advance his attack, and likewise use the webcam to siphon out stolen data."

Amazon saves user's WiFi passwords, encrypted, on their servers.

- Robert W Wishart retweeted, so I went looking in my own Alexa app



Saving Your Wi-Fi Passwords to Amazon FAQs

1. What's the benefit of saving my Wi-Fi passwords to Amazon?

Once you save your Wi-Fi passwords to Amazon, we can configure your compatible devices so that you won't need to reenter your Wi-Fi passwords on each device.

2. Will this feature work with all Wi-Fi networks?

Saving your Wi-Fi passwords to Amazon only works for secured Wi-Fi networks. It doesn't work for enterprise networks that use 802.1X authentication, hidden networks or for open networks not secured with a password.

3. Are my Wi-Fi passwords secure?

Once saved to Amazon, your Wi-Fi passwords are sent over a secured connection and are stored in an encrypted file on an Amazon server. Amazon will only use your Wi-Fi passwords to connect your compatible devices and will not share them with any third party without your permission. Amazon handles any information it receives, including your Wi-Fi passwords, in accordance with the Amazon.com Privacy NoticeAmazon.com Privacy Notice (www.amazon.com/privacy).

4. What should I do if I change my Wi-Fi passwords?

You can save your updated Wi-Fi passwords to Amazon by rerunning any compatible device through its Wi-Fi setup process. Once reconnected to your Wi-Fi network, your updated Wi-Fi password will be automatically saved to Amazon. For Dash Button, you can do this either through the Set up a Dash Button menu option within the Amazon app or by visiting amazon.com/dashbuttonsetup in your mobile browser. On Fire tablets, you can do this by going to Settings > Wireless > Wi-Fi and connecting to your desired Wi-Fi network.

5. How do I delete my Wi-Fi passwords from Amazon?

You can delete the Wi-Fi settings that you have saved to Amazon by contacting Customer Service using the Contact Us form at amazon.com/devicesupport or by phone at 1-800-273-6239 (toll free when dialing in the US). You can also delete Wi-Fi passwords saved from Fire tablets by turning off the feature on device in Settings > Backup & Restore > Save Wi-Fi Passwords to Amazon.

- Repeat after me: "Give IoT devices their own wireless network."

"You say advertising, I say block that malware"

- Forbes asked readers to turn off ad blockers then immediately served them pop-under malware.
- http://www.engadget.com/2016/01/08/you-say-advertising-i-say-block-that-malware
- Columnist "Violet Blue":
  The real reason online advertising is doomed and adblockers thrive? Its malware epidemic

is unacknowledged, and out of control.

The Forbes 30 Under 30 list came out this week and it featured a prominent security researcher. Other researchers were pleased to see one of their own getting positive attention, and visited the site in droves to view the list.

On arrival, like a growing number of websites, Forbes asked readers to turn off ad blockers in order to view the article. After doing so, visitors were immediately served with pop-under malware, primed to infect their computers, and likely silently steal passwords, personal data and banking information. Or, as is popular worldwide with these malware "exploit kits," lock up their hard drives in exchange for Bitcoin ransom.

- https://twitter.com/bbaskin/status/684067667544784897/photo/1
- -- In this instance it was a spoof of the familiar "Your JAVA is out of date and must be updated.

Et tu, Fortinet? Hard-coded password raises new backdoor eavesdropping fears

Discovery comes a month after competitor Juniper disclosed unauthorized code.

- http://arstechnica.com/security/2016/01/et-tu-fortinet-hard-coded-password-raises-new-backdoor-eavesdropping-fears/
- Reminiscent of the Juniper router backdoor... another backdoor was recently found in the older firmware of Fortinet appliances.
- In this case it's a hard-coded SSH (secure shell) password: FGTAbc11*xy+Qqz27
- Fortinet rejected the characterization of the hard-coded password as a backdoor, writing: "This issue was resolved and a patch was made available in July 2014 as part of Fortinet¹s commitment to ensuring the quality and integrity of our codebase. This was not a "backdoor" vulnerability issue but rather a management authentication issue. The issue was identified by our Product Security team as part of their regular review and testing efforts. After careful analysis and investigation, we were able to verify this issue was not due to any malicious activity by any party, internal or external. All versions of FortiOS from 5.0.8 and later as well as FortiOS 4.3.17 and later are not impacted by this issue."
- This means that the hard-coded SSH password was active in FortiOS through at least 2013 and 2014 and possibly earlier.
- No advisory from Fortinet about this was ever published.
- AND... a researcher told Dan Goodin of ArsTechnica that while the exploit no longer works as it once did, the later firmware is still suspicious because it contains the same hard-coded string!

NY State Legislator Proposes Ban On Sale Of Encrypted Smartphones

https://www.techdirt.com/articles/20160112/12590733313/ny-state-legislator-proposes-ban-sale-encrypted-smartphones.shtml

- New York Assembly Bill A8093
- http://www.nysenate.gov/legislation/bills/2015/a8093
- Relates to the manufacture and sale of smartphones that are capable of being decrypted and unlocked by the manufacturer or its operating system provider.
- Co-sponsors: Walter T. Mosley & Patricia Fahy
- From the bill: Relates to the manufacture and sale of smartphones on and after January 1, 2016 that are capable of being decrypted and unlocked by the manufacturer or its operating system provider.

Apple demands widow get court order to access dead husband's password

"Digital property after death a murky issue", says estate lawyer

- http://www.cbc.ca/beta/news/business/apple-wants-court-order-to-give-access-to-appleid-1.3405652
- Husband had a Mac he used exclusively, and they had a shared iPad.
- She knew how to unlock the iPad... but not their Apple ID.
- She could have reset the iPad... but then lost everything they had purchased.
- From the story:
  After many phone calls and two months of what [her daughter] describes as the "runaround," Donna provided Apple with the serial numbers for the items, her father's will that left everything to his wife, Peggy, and a notarized death certificate — but was told it wasn't enough.
- Donna said: "I finally got someone who said, 'You need a court order. I was just completely flummoxed. What do you mean a court order? I said that was ridiculous, because we've been able to transfer the title of the house, we've been able to transfer the car, all these things, just using a notarized death certificate and the will.
- Toronto-based estate attorney notes that there isn't any clear law.
- Apple wants a court order to protect themselves from repercussions.

Microsoft capitulates to the GWX backlash: Creates official GWX blocker.

- http://bit.ly/no-gwx
- https://support.microsoft.com/en-us/kb/3080351
- TITLE: "How to manage Windows 10 notification and upgrade options"
- SUMMARY: Qualified computers and devices that are deployed in your organization and that are running Windows 7 Pro or Windows 8.1 Pro are eligible for the free Windows 10 upgrade offer and will be able to upgrade through Windows Update. (This offer is not available to customers who are using Enterprise or Embedded editions of Windows 7 and Windows 8.1.) This article describes the notification and upgrade options, and it explains how you can manage these options.

Regardless of current disqualifying criteria, administrators who want to prevent Windows 7, Windows 7 for Embedded Systems, Windows 8.1, and Windows Embedded 8.1 Pro clients from upgrading should enable the policy settings that are discussed in this article.

- Microsoft: "Microsoft has released new updates to enable you to block upgrades to Windows 10 through Windows Update. These updates install a new Group Policy Object. Computers that have this Group Policy Object enabled will never detect, download, or install an upgrade to the latest version of Windows."

- Install an update to add a new disable GWX capability:
  - 3065987 Windows Update Client for Windows 7 and Windows Server 2008 R2: July 2015
  - https://support.microsoft.com/en-us/kb/3065987
  - 3065988 Windows Update Client for Windows 8.1 and Windows Server 2012 R2: July 2015
  - https://support.microsoft.com/en-us/kb/3065988

- Run "gpedit.msc" to launch the Group Policy Editor.
  - Under: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Update:
  - New Item: Turn off the upgrade to the latest version of Windows through Windows Update.
  - Enable that!

- Windows registry
  - To block the upgrade to Windows 10 through Windows Update, specify the following registry value:
  - Subkey: HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
    - DWORD value: DisableOSUpgrade = 1

- Hide the Get Windows 10 app (notification area icon)
  - Subkey: HKLM\Software\Policies\Microsoft\Windows\Gwx
  - DWORD value: DisableGwx = 1

- Or... just install the GWX Control Panel -- UPDATED YESTERDAY
- http://blog.ultimateoutsider.com/2015/08/using-gwx-stopper-to-permanently-remove.html
- January 18, 2016: I have just uploaded version 1.7.1.0 of the program. It has lots of usability enhancements, particularly with Monitor Mode. This version should reduce or eliminate the occasional "false alarm" alerts that happened in earlier versions, and also includes a preferences option where you can select what kinds of alerts you'd like to receive. This user guide is now up-to-date.

  Also, I am looking for information on a new kind of Windows 10 notification that Microsoft appears to be pushing out. If you have ever experienced the kind of Windows 10 desktop pop-up shown in the following picture, would you please let me know if the "Prevent Windows 10 Upgrades" feature of GWX Control Panel fixes that problem? I have never seen that notification on one of my own systems, so I am unable to test it.

Windows 10 as a service... or a disservice?

- http://www.theverge.com/2016/1/16/10780876/microsoft-windows-support-policy-new-processors-skylake
- In the Verge's words: "Microsoft says new processors will ONLY work with Windows 10"
- Windows 7 and 8.1 WON'T be updated for future processors, starting with Intel's Skylake platform

- The Verge: Soon, when you buy a new PC, it won't support Windows 7 or 8. Microsoft has announced a change to its support policy that lays out its plans for future updates to its older operating systems, and the new rules mean that future PC owners with next-generation Intel, AMD, and Qualcomm processors will need to use Windows 10.
  It's not usual for old PCs to fall short of the minimum requirements of a brand new operating system, but in this case, the opposite is happening. Microsoft and its partners will not be putting in the significant work necessary to make new hardware work with older versions of Windows. The old operating systems, at best, will merely lack the latest updates. At worst, they might not function properly.

- [Steve]: In Microsoft's Jan 13th blog posting titled "Windows 10 Embracing Silicon Innovation",
  https://blogs.windows.com/windowsexperience/2016/01/15/windows-10-embracing-silicon-innovation/
  Microsoft writes: "Going forward, as new silicon generations are introduced, they will require the latest Windows platform at that time for support. Windows 10 will be the only supported Windows platform on Intel's upcoming 'Kaby Lake' silicon, Qualcomm's upcoming '8996' silicon, and AMD's upcoming 'Bristol Ridge' silicon."

- The Verge:
  This new policy doesn't mean that Windows 7 and 8.1 are no longer supported in general. The two operating systems will continue to get updates through January 14th, 2020 and January 10th, 2023, respectively. But that's only if you're using hardware that was contemporaneous with those operating systems.

  For current PC owners, the detail to note is that Intel's current, sixth generation processors, known as Skylake, are the first that won't support either of the older versions of Windows. (Intel and Microsoft say that the platform and Windows 10 were designed for each other.) Microsoft is phasing in the policy now.

Errata

There's still life in XP... for another THREE YEARS!

- XP Embedded and XP POSReady are *different*
- XP Embedded extended support did end (with a heavy sigh) last week.
- But XP POSReady extended support continues until April 19th of 2019!
- https://support.microsoft.com/en-us/lifecycle/search/default.aspx?sort=PN&alpha=windows%20embedded%20posready%202009

Whither SN Episode #540??

- Merry Christmas! (GRC didn't relist it)

Miscellany

BRAGI UPDATE - back from Las Vegas - shipping - production
Posted by BRAGI LLC.

Dear Backer,

All units that were in transit and about to be delivered were held back by UPS (our freight forwarder). In an ispection of the goods, they discovered that the LED of Dash it is blinking in the packaging. They thought that Bluetooth was active while The Dash was blinking and stopped all shipments.

All goods are going on aircrafts, and no bluetooth is allowed to be active during flight (especially when you have thousands of devices within a pallet). UPS was correct in holding back goods. We were able to convince them that The Dash is in power save mode and not in active bluetooth mode, just because it is blinking. UPS has accepted to ship the goods after documentation on power modes from BRAGI (we had to get an employee to Hong Kong to clear the situation) and will resume shipping tomorrow.

The units that were supposed to be shipped already are being shipped to EU hub tomorrow and on Monday. Expect the previously communicated transit time. We are incredibly sorry. This is really our fault, but we didn't know that the blinking could be mistaken for active units, and didn't declare that bluetooth isn't active during blinking.

SpinRite

Jeff Rocchio in Charlotte, North Carolina
Subject: Archiving Data - Better to keep running with SpinRite or to power off?
:
This isn't so much a security question as an availability question. I've been listening to your show for about a year now; and I've been enjoying the SpinRite stories which have prompted a question: I had kids in the era of the Sony 8mm camcorder and have a bunch of videos on tape. About 2 years ago I bought two 1.5 TB hard drives, configured a Linux workstation with the necessary video software, and captured all the videos off the tapes, digitized them, and now have two copies of them all on the two 1.5 TB hard drives.

So now my question - how do I best guarantee long-term storage of these? I've thought about a cloud service, but I think the capacity I'd need to buy is a bit much. It would take too many writable DVDs to store them that way - and those can also be questionable long term. So then I thought I'd take them out of my PC, put them in thick plastic bags, and store them in the classic 'cool dry place.' But then I began to wonder about the parts degrading over time, or even the magnetism losing it's strength so that they'd become unreadable.

But leaving them running in the PC for years seems stressful as well - but if I did this with SpinRite watching them would that be better than powering them down and just leaving them sit on a shelf? What do you think?

Note: Amazon Glacier Pricing $0.007 per GB, so $7/TB/mo. $10/1.5TB/mo

---

"LostPass"

A convincing hacker-mimic of all LastPass interaction.

https://www.seancassidy.me/lostpass.html
Security researcher, Sean Cassidy, CTO of Praesidio, presented an attack at the recent ShmooCon in Washington.

He said: "I call this attack LostPass. LostPass works because LastPass displays messages in the browser that attackers can fake. Users cannot tell the difference between a fake LostPass message and the real thing because there is no difference. It's pixel-for-pixel the same notification and login screen."

From Sean's FAQ:

Why did you develop this attack?

I think that the security industry's view of phishing is naive at best, negligent at worst. Phishing is the most dominant attack vector and is used by everyone from run-of-the-mill cryptolocker types to APTs.

The standard refrain is that we need better user training. That is simply not good enough. The real solution is designing software to be phishing resistant. Just like we have anti-exploitation techniques, we need anti-phishing techniques built into more software. Software security evaluations should also include how easy it is to phish said software.

Did you tell LastPass?

Yes. I informed them in November, and they acknowledged the bug in December.
This has been a long and confusing issue. At first LastPass understood this bug to be mainly be a result of the logout CSRF. Then they suggested it wouldn't work because of the email confirmation step. The GM of LastPass said that LastPass, "can confirm this is a phishing attack, not a vulnerability in LastPass." I obviously disagree.

One of the fixes they implemented to fix LostPass was to warn users when they type in their master password into some website. However, they display a warning message in the browser viewport, like all of their messages. On an attacker-controlled website, it is trivial to detect when this notification is added. Then the attacker can do whatever. In LostPass, I suppress the notification and fire off a request to an attacker server to log the master password.
We, as an industry, do not respond to phishing attacks well. I do not blame LastPass for this, they are like everyone else. We need to take a long look at phishing and figure out what to do

about it. In my view, it's just as bad, if not worse than, many remote code execution vulnerabilities, and should be treated as such.

LastPass Immediately Responds:

"I read that LastPass is vulnerable to phishing attacks - should I be concerned?"
https://lastpass.com/support.php?cmd=showfaq&id=10072

Phishing has long been a popular tactic for trying to steal valuable information from users. On Saturday, January 16, security researcher Sean Cassidy gave a presentation at hacker convention Shmoocon demonstrating a phishing attack against LastPass. In this attack, a user is directed to a malicious website, and the page generates a notification that looks like a LastPass notification. The fake notification tricks the user into thinking they were logged out of LastPass, then directs them to login again by entering their master password, and their two-factor authentication data if they have it turned on. Although this is not a vulnerability in LastPass, we have outlined some steps below that will mitigate the risk of this and future phishing attacks.

How LastPass protects you from phishing attacks:

Preventing logout: The first line of defense that LastPass has introduced is preventing the malicious page from actually logging the user out of LastPass. Even though the malicious page shows a fake LastPass notification saying the user has been logged out and needs to login again, the user can see that the LastPass extension itself in their browser toolbar is still logged in.

What if the user misses that they're still logged in to LastPass and clicks on the fake LastPass notification to login again?

Warning that the master password was entered on a non-LastPass page: LastPass will detect if the user enters their master password on a non-LastPass page and pops a strong warning, even before the user submits it to the page.* The user will know immediately that their master password may have been compromised and can change it.

But what if the malicious page suppresses that warning from LastPass, so the user still enters their master password, and potentially their two-factor authentication data?

Requiring verification for logins from unknown locations or devices: LastPass has a verification process that is required whenever a user attempts to login from an unknown location or device. Cassidy claims in his research that it is possible for the malicious page to suppress any messages LastPass tries to show in the viewport, thereby potentially preventing the user from seeing the above master password warning. So if the user does not see the warning, and still enters their master password and their two-factor data, the attacker could then attempt to remotely login to their LastPass account. However, upon attempting to login, they would

be unable to gain access to the account without also completing the email verification steps. This requires access to the user's email address (or security email address, if enabled for their LastPass account) to approve the new location or device.

The verification process significantly reduces the threat of this phishing attack. The attacker would need to gain access to the user's email account as well, which could also be mitigated by two-factor authentication for their email account. Should a user see a verification request that they did not initiate, they can safely ignore it. Out of caution, we recommend updating the master password as well in the LastPass Vault by launching Account Settings and entering a new master password, then saving your changes.

Requiring verification even for accounts with two-factor authentication: Previously, LastPass allowed users with two-factor authentication turned on to bypass the verification process, as they already had additional protection enabled for their account. We have now changed the default so that all users, even those with two-factor authentication, will be directed to the verification process when logging in from unknown devices or locations.

Warning against master password reuse: LastPass also alerts users when it detects that their master password is being used as a password for other websites. LastPass performs this check locally, on the user's device, so the master password is never sent to LastPass and no sensitive information is disclosed to LastPass. The user is then advised to update their passwords and to be careful to never reuse their master password.

Revisiting our notification approach: To date, LastPass has relied on the viewport for notifications. This is the area below the tab bar and URL address bar, where web pages normally appear in the browser. LastPass has significant measures in place to protect our usage of viewports using iframes, but our team is working to release additional notification options that bypass the viewport and therefore eliminate the risk that it presents in phishing attacks.

Looking to the browser for better protection:

A point that was only briefly raised in Cassidy's research was the role that the browser itself plays in this attack. LastPass has encouraged Google for years to provide a way to avoid using the browser viewport for notifications. As a true solution to this threat, Google should release infobars in Chrome that give extensions the capability to do proper notifications outside the DOM. You can see our plea for this back in January 2012 with still no resolution; please star this issue to help us raise awareness.

We hope that future improvements to the browser will help us go even further to protect users from these types of attacks. In lieu of that possibility right now, though, we have taken other steps to strengthen LastPass.