Security Now! #546 - 02-09-16

Router Q&A Follow-up

This week on Security Now!

- An interesting Apple 3rd-party service conundrum.
- Comodo's Crummy Cromodo Browser.
- A new Google search safely feature.
- An interesting audit of Window 10 after enabling all privacy features.
- My experience with GWX and a new Win7 install.
- The amazing clever hack of the decade.
- Some quick Zeo and other miscellany.
- Three listener follow-up questions from last week's "Three Dumb Routers" episode.

Security News:

iOS Error 53:
Error 53: Apple remotely bricks phones to punish customers for getting independent repairs
Cory Doctorow / BoingBoing
http://boingboing.net/2016/02/05/gerror-53-apple-remotely-bric.html

<quote> According to an Apple spokesperson, Error 53 is an anti-tampering measure designed to protect the integrity of the phone's biometric security system. The lockout is designed to protect users from trusting doctored fingerprint readers that might allow unauthorized access to their phones.

But the phones that Apple is remote-killing haven't been doctored: they've been fixed. There are many independent service centers for Apple's products where you can get your phone fixed more cheaply than the official rate. Independent service centers also thrive in places where there are no Apple service centers at all.

Comodo doesn't respond so Google goes public about "Chromodo":
https://code.google.com/p/google-security-research/issues/detail?id=704
Comodo "Chromodo" Browser disables same origin policy, Effectively turning off web security.
https://www.comodo.com/home/browsers-toolbars/chromodo-private-internet-browser.php

- Comodo: "Chromodo Private Internet Browser"
  Fast and versatile Internet Browser based on Chromium, with highest levels of speed, security and privacy!

- Google's Tavis Ormandy is at it again.
  - <quote> When you install Comodo Internet Security, by default a new browser called Chromodo is installed and set as the default browser. Additionally, all shortcuts are replaced with Chromodo links and all settings, cookies, etc are imported from Chrome. They also hijack DNS settings, among other shady practices. Chromodo is described as "highest levels of speed, security and privacy", but actually disables all web security. Let me repeat that, they ***disable the same origin policy***.... ?!?..

- Same Origin Policy: (utterly rigid domain stovepiping)
  - Script from one origin domain can ONLY ACCESS assets from that same origin domain. If that is not enforced there is NO security.

Google begins blocking websites containing deceptive content
http://arstechnica.co.uk/information-technology/2016/02/google-now-blocking-websites-that-show-fake-download-buttons/

Google has started blocking websites that use deceptive content or ads to make you do things you wouldn't normally do, such as fake download buttons that appear right next to the real download button, or pop-ups informing you that you need to download an updated media player to view the site's content.

It will be a gradual rollout.

The blocking will occur via Google's Safe Browsing tech, the full page warning that appears when you click on a potentially unsafe search result.

Safe Browsing has been around for years, but it mostly prevented us from visiting sites that were serving up malware, or sites that Google had otherwise deemed unsafe.

In November Google began blocking sites that used "social engineering attacks" to get you to install unwanted software or reveal sensitive information—and today, Google is expanding that to websites that serve up deceptive embedded content (i.e. adverts).

Following Amazon, Google's Chrome browser will start blocking all FLASH content that isn't "central to the webpage" on September 1st.
http://arstechnica.co.uk/information-technology/2015/08/google-chrome-will-block-auto-playing-flash-ads-from-september-1/

Flash content, such as ads or auto-playing videos on non-video websites, will be automatically paused by default—but you can click to play them if you wish. Embedded video players on sites like YouTube and Vimeo will still work, of course.

The Flash-blocking feature was initially rolled out in a beta release of Chrome earlier this year.

Google's Tommi Li stated that the reason for the blocking was battery life because auto-playing

Flash ads consume a large amount of CPU and energy.

(Steve Jobs' refusal to host FLASH on iOS seems more prescient everyday.)

The majority of online advertising still makes use of Flash, even on mobile, where Flash has never been fully supported.

A recent report by mobile ad management firm Sizmek (PDF) stated that advertisers tried to deliver more than 5.35 billion Flash ads in Q1 2015—which ended up defaulting to static images—versus 4.25 billion HTML5 ads.

Remember: Amazon's updated guidelines also state that they will also stop accepting FLASH ads on September 1st.

Even with Telemetry Disabled, Windows 10 Talks to Dozens of Microsoft Servers
http://slashdot.org/submission/5534447

- Curious about the various telemetry and personal information being collected by Windows 10, one user installed Windows 10 Enterprise and disabled all of the telemetry and reporting options. Then he configured his router to log all the connections that happened anyway. Even after opting out wherever possible, his firewall captured Windows making around 4,000 connection attempts to 93 different IP addresses during an 8 hour period, with most of those IPs controlled by Microsoft. Even the enterprise version of Windows 10 is checking in with Redmond when you tell it not to — and it's doing so frequently.

Windows 10 telemetry network traffic analysis, part 1:
Posted by "CheesusCrust"
https://voat.co/v/technology/comments/835741

- Like many of you, I am concerned about the telemetry, spying and other surveillance features, known or unknown, of Windows 10. It has concerned me enough to push me to Linux Mint as my main operating system. Even so, I wanted to better understand Windows 10, but internet search results for a decent windows 10 traffic analysis leave a lot to be desired. As such, I decided to do my own investigating of what, exactly, Windows 10 is doing traffic-wise, and post the results. For this analysis, I wanted to simply analyze the network traffic of Windows 10 on a clean install, and just let it sit and run without using it.

What I have done for this analysis:

- I have installed DD-WRT on a router connected to the internet and configured remote logging to the Linux Mint laptop in #2.
- I have installed Linux Mint on a laptop, and setup rsyslog to accept remote logging from the DD-WRT router.
- I have installed Virtualbox on the Linux Mint laptop, and installed Windows 10 EnterprisePNG on Virtualbox. I have chosen the customized installation option where I disabled three pages of tracking options.
- I have configured the DD-WRT router to drop and log all connection attempts via iptables through the DD-WRT router by Windows 10 Enterprise.

- Aside from installing Windows 10 Enterprise, and verifying the internet connection through ipconfig and ping yahoo.com, I have not used the Windows 10 installation at all (the basis for the first part of this analysis)
- Let Windows 10 Enterprise run overnight for about 8 hours (while I slept).
- I use perl to parse the data out of syslog files and insert said data into a Mysql database.
- I use perl to obtain route data from whois.radb.net, as well as nslookup PTR data, and insert that into the Mysql database.
- Lastly, I query and format the data for analyzing.

Here is the roughly 8-hour network traffic analysis of 5508 connection attempts of an unused, base install of Windows 10 Enterprise (NOTE: I did not remove any 192.168.1.x home network IP addresses from the analysis):
https://voat.co/v/technology/comments/835741

Steve's experience with GWX and a new Win7 setup

John McCain's guest editorial in Bloomberg View (last Friday, Feb 5th).
http://www.bloombergview.com/articles/2016-02-05/silicon-valley-should-join-the-war-on-terrorism

- A predictable anti-Obama political component.
- Completely ignores the fact that encryption is already a 3rd-party add-on.
- And let's also remember that Metadata and Content are fundamentally different.
    - While encryption can robustly protect the content of conversations, nothing about the Internet protects the evidence of that communication. The difficulties of making TOR work demonstrate this difficulty.

Amazing hack of the decade
http://blog.checkpoint.com/2016/02/02/ebay-platform-exposed-to-severe-vulnerability/
<quote> Check Point has discovered a severe vulnerability in eBay's online sales platform. This vulnerability allows attackers to bypass eBay's code validation and control the vulnerable code remotely to execute malicious Java script code on targeted eBay users. If this flaw is left unpatched, eBay's customers will continue to be exposed to potential phishing attacks and data theft.

An attacker could target eBay users by sending them a legitimate page that contains malicious code. Customers can be tricked into opening the page, and the code will then be executed by the user's browser or mobile app, leading to multiple ominous scenarios that range from phishing to binary download.

After the flaw was discovered, Check Point disclosed details of the vulnerability to eBay on Dec 15, 2015. However, on January 16, 2016, eBay stated that they have no plans to fix the vulnerability. The exploit Demo is still live.

The Vulnerability:

Check Point security researcher Roman Zaikin recently discovered a vulnerability that allows attackers to execute malicious code on eBay users' devices, using a non-standard technique called "JSF**k." This vulnerability could allow cyber criminals to use eBay as a phishing and malware distribution platform.

To exploit this vulnerability, all an attacker needs to do is create an online eBay store. In his store details, he posts a maliciously crafted item description. eBay prevents users from including scripts or iFrames by filtering out those HTML tags. However, by using JSF**k, the attacker is able to create code that will load additional JS code from his server. This allows the attacker to insert remotely sourced and controllable JavaScript that he can adjust to, for example, create multiple payloads for a different user agent.

eBay performs simple verification, but only strips alpha-numeric characters from inside the script tags. The JSF**k technique allows the attackers to get around this protection by using a very limited and reduced number of characters.

The technique was invented by Martin Kleppe.

- It uses only 6 non-alphanumeric characters []()!+ to bypass most forms of payload sanitation.
- The following basic vocabulary helps us write anything we need:
  - [and] – Access array elements, objects properties, get numbers and cast elements to strings.
  - (and) – Call functions and avoid parsing errors.
  - + – Append strings, sum and cast elements to numbers.
  - ! – Cast elements to Booleans.

- How to use it:
  - To get a numeric zero (0): +[] (The first value from an empty list is 0)
  - To get True or False, we cast those to Boolean:
    - ![] yields false
    - !![] yields true
  - Casting 'true' to an integer yields 1
    - +!![]
    - Or to get "1" as a string: +!![]+[]
  - To get a longer number, we create the digits and translate into an integer:
    - +((+!![]+[])+(!+[]+!![])+(!+[]+!![]+!![]+[])) yields the integer: 123

  - And so forth…
    We can get letters and all sorts of other intermediates from combinations

Errata

- It's an Ethernet "Frame" not a "Packet"

Miscellany

Zeo True-EEG Sleep Manager Pro **///** 100, 355, 460 (915)
Good Morning Steve,

Yes this is an awesome phenomenon, We only have matched sets right now, we do not have any more single headbands.

I did post another 460 this morning, that is an accurate number for listing as we are counting daily so we do not over sell this product. I think there are another 300+ after the 460 but I need them counted to be sure.

I just wanted to give you heads up that we so appreciate your work and "advertising" for us that we are sending you a thank you package. We know we do not have to but we want to and show our appreciation for your like of the product and letting people know about it. We did not raise the price as we want you to have credibility with your listeners and give them a great deal.

Thank you very much for the broadcast and we are trying to make all your listeners happy, we do not usually ship out of the US but you have a few followers in the UK, Canada, Brazil and Australia that would like them. We are making special arrangements for these followers.

Thank you again,

I would like you to know we are a team here and with Angie, Jose, Chad and Angela's help we are getting these packages out in a timely manner.

Dawn Ames | Asset Sales Supervisor

- MUST clean the pads
- Amazon FIRE on sale $40 through Feb 13th.

"The Expanse"
Was SO GOOD that I started wishing that I hadn't read the books.

Fusion Updates:

- December 10th, Germany:
- Wendelstein 7-X (W7-X)
- Stellarator.
- 80 billion degrees for 1/4 second
- February 8th, China:
- Experimental Advanced Superconducting Tokamak (EAST)
- Traditional Tokamak fusion bottle
- 50 million degrees for 102 seconds.
- http://www.sciencealert.com/china-s-nuclear-fusion-machine-just-smashed-germany-s-hydrogen-plasma-record

SpinRite

<< Initial contact eMail >>

Greg replies:
Do you have an internal SATA drive??

If so, in your motherboard BIOS settings, you will likely find an option to switch your SATA motherboard to something called "Legacy IDE" or "Legacy Operation" or "Compatibility Mode" or even simply "ATA" or "IDE". Various BIOSes call it different things, but the idea is that the SATA controllers are made to appear as standard, traditional IDE ATA drives. We have encountered instances where the newer SATA BIOS ode was less well tested than the older and more solid Legacy code which SpinRite uses. You should restore your motherboard to its previous SATA setting once you're done running SpinRite on your SATA drives.

Forrest's first reply:
Greg,
Thank you. I'll make the suggested changes to the BIOS and start SpinRite again.
Thank you!
--Forrest

Hello,

I wanted to let you know that the BIOS ATA settings allowed SpinRite to run… and it worked!

I was able to recover the pictures my daughter had taken around Europe in the Fall of 2014 when she was doing a Study Abroad her Junior year of college. Now she'll be getting the pictures for her Valentine's Day present! She studied Marketing overseas and as a Photography Major she was very disappointed when the last week of her semester the hard drive "crashed".

I had been saving up money to send the drive off to a data recovery group. Thanks to SpinRite, that wasn’t necessary. Now she can add a few of the pictures to her web site.

Thank you for creating a great tool!

--Forrest

Q&A

NateSmith (@n8person)
Hi Steve!
Could I open up some ports on the "IoT" router and 'reach in' from within the private LAN? Seems like NAT on the root router would push a request over to the IOT modem's WAN IP. Does this break anything?

(Notes: Let's talk in much more detail about IP-routing among networks.)

Ken Hundley (@KenHundley)
Hi Steve. Your Three Dumb Routers podcast answered several questions I had about this but I have one more that I'm hoping you can answer and "may" be something worth mentioning on your show (maybe not). I have a 4th router that I need. It's required by Comcast for their Home Security system and I have no access or control over it. With this setup I would have at least 3 wireless routers. Will I run into any potential issues having so many wireless networks in such a small area? Thanks!

Yuki Takizawa (@yukitz)
Hi Steve, I just listened to the 3 dumb routers episode. So I just wanted to DM you a quick question: I get the isolation property with any of these approaches. My #1 issue is sharing a printer on my home network among secure & 'guest' networks. Perhaps a more sophisticated VLAN routing software/configuration could do this, but it seems hard with a simple setup, even if I use multiple routers.