Security Now! #472 - 09-09-14

Q&A #196

Link Tracking Warning!
This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

This week on Security Now!

- If it's the second Tuesday of the month... we know what that means.
- Interesting and disturbing news of the Home Depot breach.
- Comcast gets pretty intrusive.
- Google declares war on the SHA-1 hash.

Security News:

Patch Tuesday

- The tamest in a long while.
- One "Critical" IE-based publicly-disclosed remote code execution vulnerability.
    - (And 36 privately reported less critical vulnerabilities.)
- One "Important" .NET DoS vulnerability.
    - Only possible if user installed and registered ASP.NET on their machine.
- A Windows 8 Elevation of Privilege in Windows Task Scheduler.
    - Attacker must logon locally to a vulnerable machine with valid logon credentials.

Add Home Depot to the "massive credit card breach" list

- Home Depot confirms: US & Canadian Purchases since April VULNERABLE.
- Brian Krebs reports that despite HD's quick claim that no debit card PIN data was stolen, multiple financial institutions are reporting s steep upswing over the past few days in fraudulent ATM withdrawls.
- What was stolen? The card data stolen from Home Depot customers (and now being offered for sale on the crime shop "Rescator.cc") includes all of the information needed to fabricate counterfeit cards, as well as the legitimate cardholder's full name and the city, state and ZIP of the Home Depot store from which the card was stolen. This additional information allows bad guys to perform enough research on individual victims to then obtain enough additional information to use the victim's bank automation to change the "forgotten" PIN number to one of their choosing... and thereby enable the use of ATMs for cash withdrawl.
- For example, Brian reported that he heard from the manager of a large West Coast bank that lost more than $300,000 in two hours yesterday to PIN fraud on multiple debit cards that had all been used recently at Home Depot. The manager said the bad guys called the customer service folks at the bank and provided the last four digits of each cardholder's Social Security number, date of birth, and the expiration date on the card. And that was enough information for the bank to reset the customer's PIN.

- The SAME Malware: The breach appears to have been enabled by a variant of the SAME MALWARE that claimed Target as its victim last December. At least some of the Home Depot store registers had been infected with a new variant of the "BlackPOS" malware strain.

Comcast Xfinity Wi-Fi hotspots performs JavaScript injection.

- What the user receives is not what the server sent.
- Hard to sympathize, though, when so many pages are pulling content from dozens of other servers already.

Google pushes for the end of SHA-1

- http://blog.chromium.org/2014/09/gradually-sunsetting-sha-1.html
- https://groups.google.com/a/chromium.org/forum/#!topic/security-dev/2-R4XziFc7A[51-75-false]
- <quote> We plan to surface, in the HTTPS security indicator in Chrome, the fact that SHA-1 does not meet its design guarantee. We are taking a measured approach, gradually ratcheting down the security indicator and gradually moving the timetable up.
- Other browsers?
    - Microsoft already announced their 2017 intentions
    - Opera: Announced they're following Google
        - "Although we do understand some of the problems this causes for the CAs, Opera fully backs Chromium on this issue. We plan to follow and implement the same behavior."
    - Safari & Mozilla: Standing by and watching the fur fly.

Errata:

USB *IS* Differential

- 4-conductors, +5, Gnd, S+, S-

SpinRite: Cedric McGraw in Moncton, NB, Canada

Hello Steve and Leo,

I'm a long time listener and I think the show is fantastic. I'm a high school IT teacher and I incorporate your show in my classroom every week. The students love talking about security issues.

I have a quick question about SpinRite. Is there any benefit to running SpinRite on an empty drive? For example, if I use DBAN on an older drive, is there any advantage to running SpinRite before installing the OS?

Thank you for the great education you provide your listeners week after week.