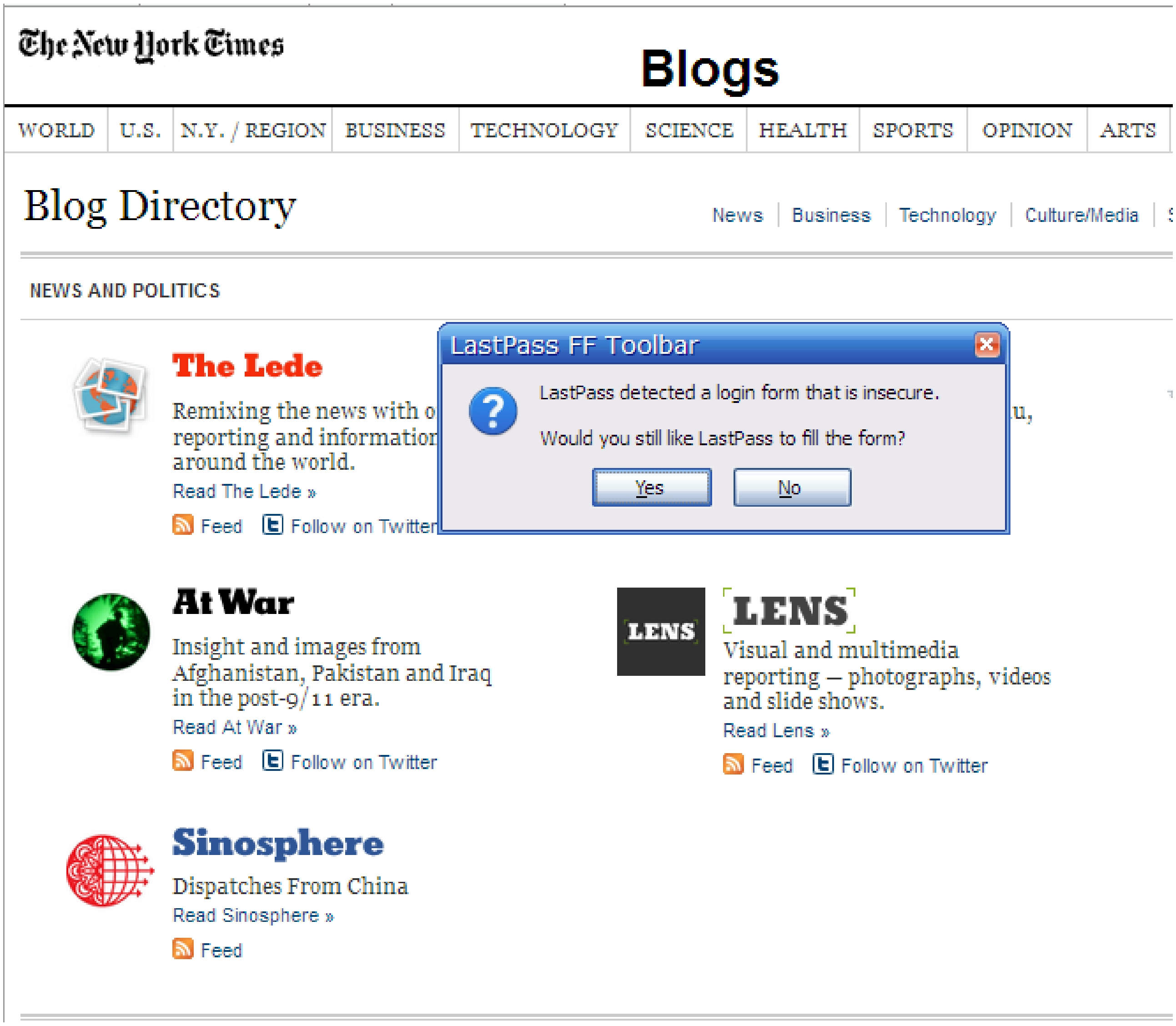
Security Now! #463 - 07-08-14
Q&A #191

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!

- Microsoft's Patch Tuesday & they fumble a takedown
- Oracle ends XP's Java
- Google finds unauthorized certs in the wild
- A cautionary tale about "The Internet of Things"
- SN: Cloud Storage Solutions update
- Miscellania... and our listener Q&A



The New York Times

Blogs

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS

Blog Directory

News | Business | Technology | Culture/Media |

NEWS AND POLITICS

The Lede

Remixing the news with o
reporting and informatior
around the world.
Read The Lede »
Feed Follow on Twitter

LastPass FF Toolbar

LastPass detected a login form that is insecure.

Would you still like LastPass to fill the form?

Yes No

At War

Insight and images from Afghanistan, Pakistan and Iraq in the post-9/11 era.
Read At War »
Feed Follow on Twitter

LENS

Visual and multimedia reporting – photographs, videos and slide shows.
Read Lens »
Feed Follow on Twitter

Sinosphere

Dispatches From China
Read Sinosphere »
Feed

Security News:

Microsoft's Patch Tuesday

- 2-Critical (Remote Code Execution), 3-Important, 1-Moderate

- MS14-037 - IE: CRITICAL / Remote Code Execution
  Cumulative Security Update for Internet Explorer (2975687)
  This security update resolves one publicly disclosed vulnerability and twenty-three privately reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

- MS14-038 - Windows: CRITICAL / RCE
  Vulnerability in Windows Journal Could Allow Remote Code Execution (2975689)
  This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

- Important:
  - Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege
  - Vulnerability in Ancillary Function Driver (AFD) Could Allow Elevation of Privilege (2975684)
  - Vulnerability in DirectShow Could Allow Elevation of Privilege (2975681)
- Moderate:
  - Vulnerability in Microsoft Service Bus Could Allow Denial of Service (2972621)

NoIP - Microsoft's Clutzy Takedown

- More than 4 MILLION website domains went dark
- https://www.noip.com/blog/2014/06/30/ips-formal-statement-microsoft-takedown/
- (Monday, June 30th) We want to update all our loyal customers about the service outages that many of you are experiencing today. It is not a technical issue. This morning, Microsoft served a federal court order and seized 22 of our most commonly used domains because they claimed that some of the subdomains have been abused by creators of malware. We were very surprised by this. We have a long history of proactively working with other companies when cases of alleged malicious activity have been reported to us. Unfortunately, Microsoft never contacted us or asked us to block any subdomains, even though we have an open line of communication with Microsoft corporate executives.

  We have been in contact with Microsoft today. They claim that their intent is to only filter out the known bad hostnames in each seized domain, while continuing to allow the good hostnames to resolve. However, this is not happening. Apparently, the Microsoft infrastructure is not able to handle the billions of queries from our customers. Millions of innocent users are experiencing outages to their services because of Microsoft's attempt to remediate hostnames associated with a few bad actors.

Had Microsoft contacted us, we could and would have taken immediate action. Microsoft now claims that it just wants to get us to clean up our act, but its draconian actions have affected millions of innocent Internet users.

Vitalwerks and No-IP have a very strict abuse policy. Our abuse team is constantly working to keep the No-IP system domains free of spam and malicious activity. We use sophisticated filters and we scan our network daily for signs of malicious activity. Even with such precautions, our free dynamic DNS service does occasionally fall prey to cyber scammers, spammers, and malware distributors. But this heavy-handed action by Microsoft benefits no one. We will do our best to resolve this problem quickly.

- (Thursday, July 3rd) We would like to give you an update and announce that ALL of the 23 domains that were seized by Microsoft on June 30 are now back in our control. Please realize that it may take up to 24 hours for the DNS to fully propagate, but everything should be fully functioning within the next day. One of the domains, noip.me, took longer to get back online, but it should be fully restored within the next day. Is your service back up? Please send us a tweet and let us know.

  We are so sorry for the inconvenience that this takedown has caused our customers. Thank you so much for the support and for sticking with us through the entire process this week. More information surrounding this event will be released within the next few days, so stay tuned.

  Again, THANK YOU.

Oracle suspends support for JAVA... or do they?

- http://www.zdnet.com/java-support-over-for-windows-xp-7000031226/
- <ZD Net quote> The regularly scheduled quarterly security updates for Java on July 15 will not include updates for Windows XP, which is now formally unsupported by Oracle.
- Henrik Stahl, vice president for product Management at Java:
  "As you know, Microsoft no longer supports Windows XP and recommend their users to upgrade to more recent versions in order to maintain a stable and secure environment. Oracle makes the same recommendation to our users running Java on Windows, and also has a standing recommendation that users stay current with the most recent Java security baseline — currently available for the public for Java 7 and 8. There are a few compatibility issues with Java 8 on Windows XP, since it is not an officially supported configuration. We are looking at ways to resolve these.
  For now, we will keep Java users on Windows XP secure by updating them to the most recent Java 7 security update on an ongoing basis. Java users on more recent Windows versions can choose between Java 7 and 8, and depending on their choice will be kept up to date with the most recent Java 7 or 8 security update respectively."

Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords

- http://arstechnica.com/security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/
- What Happened?
  - Security by Obscurity -- worth doing, but can never be enough by itself.
  - Hackers figured out how to reverse-engineer the chips using JTAG debuggers.
  - Extracted the code and found the FIXED AES cipher key used between devices.
  - Encrypted in the statically-keyed data was the network's secret WiFi password.
- What can we do?
  - ONLY run "Internet Things" on a bifurcated network with separate passwords.

Google blocks unauthorized Indian Certs for Google domains:

- http://googleonlinesecurity.blogspot.com/2014/07/maintaining-digital-certificate-security.html
- http://boingboing.net/2014/07/08/fake-google-subdomain-certific.html
- An Indian CA trusted by (only) Microsoft has been caught issuing fake Google subdomain certificates that would allow nearly undetectable eavesdropping on "secure" connections to services like Google Docs.
- Google caught them, notified everyone, and pushed a change to their CRLSet.
- I now watch Chrome's CRLSets, so I caught the change instantly:
  - https://www.grc.com/groups/sqrl:6527

SN: Cloud Storage Solutions

- An *amazing* Wikipedia page already exists:
- Comparison of online backup services
- https://en.wikipedia.org/wiki/Comparison_of_online_backup_services

Miscellany

Silent Circle not by Moxie Marlinspike, it's by Phil Zimmerman

Extant Premieres tomorrow (Wednesday) on CBS

Tango PC

- http://bgr.com/2014/07/07/tango-pc-hands-on-preview/
- https://www.kickstarter.com/projects/tiny/tango-super-pc-a-desktop-windows-pc-in-cell-phone
- 67 hours to go...

SQRL:

"bothyhead" (@bothyhead) @ 4:38am · 8 Jul 2014 via Plume for Android:
@SGgrc I've just been playing with Ralf's SQRL client and his test site. I so hope this takes off; it's amazing. The world owes you one :-)

(Notes: Ralf - GSM/OCB - Soft Spec…)

SpinRite:

Kevin Marken in Calgary, AB Canada
Subject: Spinrite on Bitlocked drive

Hi Steve, I listen to Security Now every week. I have looked a bit but have now found anything about how SpinRite will handle a Microsoft Bitlocked drive. Can SpinRite work the same on a bitlocked drive as a non-bitlocked drive? Can I run spinrite against a Bitlocked drive? Kevin