Security Now! #564 - 06-14-16

Q&A #235

This week on Security Now!

- BlueCoat Systems gets a new parent
- A bad Chrome bug you never knew you had
- More news from the hacker "Peace"
- LetsEncrypt's mass eMailer reveals a fun bug
- Another "What is Microsoft thinking?" revelation
- Revisiting a Sci-Fi author
- Ten questions and comments from our terrific listeners

Security News

Patch Tuesday: More than 36 security vulnerabilities addressed!

- (Abobe delaying Critical FLASH update to address active attack.)

Symantec to buy Blue Coat for $4.65 Billion

- Last year Bain Capital purchased BlueCoat for $2.4 billion.
- Symantec announced overnight that it had just purchased BlueCoat from Bain for $4.65 billion.
- @SwiftOnSecurity: With Symantec's acquisition of Blue Coat, a root Certificate Authority will now be selling carrier-grade SSL decryption solutions to governments worldwide.
- What does this mean??... connection encryption had a brief shining moment...

Google Chrome fixed a frightening bug in its integrated PDF viewer

- Cisco's Talos security group found and reported a remote code execution vulnerability.
- http://blog.talosintel.com/2016/06/pdfium.html
- PDFium is Chrome's built-in PDF reader. Talos identified an exploitable heap buffer overflow vulnerability in the PDFium PDF reader. By simply viewing a PDF document that includes an embedded jpeg2000 image, the attacker can achieve arbitrary code execution on the victim's system. The most effective attack vector is for the threat actor to place a malicious PDF file on a website and then either offer the PDF for viewing or via phishing emails or even malvertising.
- Although the trouble is in the OpenJPEG library, the stand-alone build of OpenJPEG doesn't have this problem due to the presence of some assertions which Google's Chrome missed due to its special build process and execution environment.

Hacker "Peace" has another 51 million account credentials to sell

- http://thehackernews.com/2016/06/imesh-data-breach.html
- "Peace" (who was selling the 117 additional LinkedIn account credentials) now has (and is also offering for sale) 51 million account credentials obtained from iMesh, a peer-to-peer file sharing service which was launched in 2009 and shut down last month.
- The database contains email addresses, usernames, passwords, IP addresses, location information and other information on users.
- The passwords were all hashed and salted... but unfortunately with MD5... which doesn't pose much barrier for someone wishing to bruce-force the password data.
- The data is for sale on the dark web for just 0.5 Bitcoin (nearly US$335).

The prolific hacker "Peace of Mind" -> Peace

- https://www.wired.com/2016/06/interview-hacker-probably-selling-password/
- "An Interview With the Hacker Probably Selling Your Password Right Now"
- "TheRealDeal" dark web marketplace
- Seller (Peace) has a 100% satisfaction rating, "A+++" feedback, and "follows up with questions and delivers promptly."
- Peace's growing inventory of "merchandise" includes:
    - 167 million user accounts from LinkedIn,
    - 360 million from MySpace,
    - 68 million from Tumblr,
    - 51 million from iMesh,
    - 71 million from Twitter,
    - 100 million from the Russian social media site VK.com.

- During the Wired conversation:
    - Well, these breaches were shared between the team and used for our own purposes. During this time, some of the members started selling to other people. The people who we sold to were selective, not random or in public forums and such, but only to people who would use the data for their own purposes and not resell or trade.
    - However, after enough time went by, certain individuals who had obtained the data started to sell it in bulk ($100/100k accounts, etc.) to the public. After noticing this, I decided to start making a little extra cash to start selling publicly, as well.
    - Wired: "Why didn’t the crew want to sell the whole collection earlier?"
    - "It is not of value if data is made public. We had our own use for it, and other buyers did as well. In addition buyers expect this type of data to remain private for as long as possible. There are many databases not made public for that reason and in use for many years to come.
    - Wired: What was your “own use” for it? How were you able to make more by selling the data privately?
    - Well, the main use is for spamming. There is a lot of money to be made there, as well as in selling to private buyers looking for specific targets. As well, password reuse—as seen in recent headlines of account takeovers of high profile people. Many simply don’t care to use different passwords which allows you to compile lists of Netflix, Paypal, Amazon, etc. to sell in bulk. (50K/100K/etc)
    - Lists tend to sell from $15K, $10K, down to a few $k.

The mass eMailer used by LetsEncrypt had an intriguing bug...
https://community.letsencrypt.org/t/email-address-disclosures-preliminary-report-june-11-2016/1686
LetsEncryt Explains:
On June 11 2016 (UTC), we started sending an email to all active subscribers who provided an email address, informing them of an update to our subscriber agreement. This was done via an automated system which contained a bug that mistakenly prepended between 0 and 7,618 other email addresses to the body of the email. The result was that recipients could see the email addresses of other recipients. The problem was noticed and the system was stopped after 7,618 out of approximately 383,000 emails (1.9%) were sent.

Each email mistakenly contained the email addresses from the emails sent prior to it, so earlier emails contained fewer addresses than later ones.

We take our relationship with our users very seriously and apologize for the error. We will be doing a thorough postmortem to determine exactly how this happened and how we can prevent something like this from happening again. We will update this incident report with our conclusions.

If you received one of these emails we ask that you not post lists of email addresses publicly.

Visual Studio 2015 C++ Compiler Secretly Inserts Telemetry Code Into Binaries
https://yro.slashdot.org/story/16/06/10/1350245/visual-studio-2015-c-compiler-secretly-inserts-telemetry-code-into-binaries
https://www.infoq.com/news/2016/06/visual-cpp-telemetry
http://news.softpedia.com/news/visual-studio-2015-secretly-inserts-telemetry-code-into-c-plus-plus-binaries-505113.shtml
<Headline Quote>
Internet users have pulled out the pitchforks and are once again at odds with Microsoft regarding telemetry data, but this time around, it's because the company updated Visual Studio 2015, which is now adding secret telemetry code in the C++ binaries compiled by every developer.

The issue surfaced in May on Reddit, when a user noticed a function named "telemetry_main_invoke_trigger" added to every binary he compiled for his private projects.

The user tested and discovered this happening with Debug and Release-level binary builds, on both Windows 7 and Windows 10.

What worried Reddit users was that there was no documentation for these calls, either online or in the software's built-in documentation package. As we know... "Telemetry data" is a potential sore point with Microsoft users, and most people jumped to the conclusion that this was yet another method through which Microsoft adds telemetry calls to spy on users and the way they use their software on Windows.

However... Steve Carroll, one of the high-ranking managers for the Visual Studio team, answered everyone's questions regarding this undocumented feature:

Steve wrote: "Our intent was benign - our desire was to build a framework that will help investigate performance problems and improve the quality of our code optimizer should we get any reports of slowdowns or endemic performance problems in the field. We apologize for raising the suspicion levels even further by not including the CRT (Common RunTime) source, this was just an oversight on our part."

Next Week: Deep propeller-head episode -> Intel's forthcoming Control-Flow Enforcement Technology (CET)

This Week in SQRL

Chris M. in Tennessee asks:

Hi Steve! Love the podcast and a proud owner of SpinRite.

I have a question about SQRL compatibility: Will all websites work with it? or will each individual site have to turn something on for it to work? Does it work with applications or is it solely a website thing?

For example will it work with the Dropbox or Google drive applications on windows?

I got excited when I heard you talk about it but then I started thinking that I misunderstood what it is.

Thanks!

Miscellany

AMAZING DigiCert EV Certificate Experience on a Sunday night at 7:30pm.

An update and recommendation on Richard Philips "Rho Agenda" series

- Orson Scott Card: (Enders Game): "I promise you that Richard Phillips is going to be a popular and influential writer, period. As good as any science fiction being written today."
- http://secondship.com/
- The Rho Agenda trilogy: Second Ship, Immune, Wormhole
- Jack & Janet: Once Dead, Dead Wrong, Dead Shift
- The next Trilogy: The Kasari Nexus, The Altreian Enigma, The Meridian Ascent
- ALL eBooks: "KindleUnlimited" -- read for free!

(I'm now reading "The Great North Road" (Peter F. Hamilton))

SpinRite

Daniel Hankins
Location: Scottsdale, Arizona
Subject: Does Spinrite mask impending catastrophic failure?

I run Spinrite in maintenance mode on all my drives a few times a year. Then I had a thought: How am I to know when a drive needs replacing?

If Spinrite keeps fixing up a drive that's becoming increasingly marginal, the first warning I'm likely to get is when the frequency and density of errors overwhelms Spinrite's ability to correct them.

At that point, wouldn’t I be left with a “used up” drive that even Spinrite can't fix??

If I'm using Spinrite to keep my drives running smoothly, what should I look for to tell me when it's time to retire a drive?