Security Now! #521 - 08-18-15

Security is Difficult

This week on Security Now!

- Android StageFright, two steps forward, one step back
- Windows 10 new privacy concerns
- High profile Malvertising surfaces
- Kaspersky, Lenovo, HTC and AT&T each in their own doghouses.
- Some miscellaneous tidbits...
- Some additional thoughts about surfing safety and web advertising.

Security News

Android StageFright:

- First the good news: Phones are getting patched and reporting non-vulnerable.
- Ernest Koch @nullconmedia
  - @SGgrc After yesterday's patch, my Nexus 6 is showing not vulnerable.
- Simon Zerafa confirmed that both his Nexus 6 & 7 were just updated.
  - Nexus 6 Android 5.1.1 build LMY48I gets 6 greens on the Zimperium StageFright test :-)
- Joe McDaniel @joem5636
  - @SGgrc just got my Nexus 5.1.1 upgrade. Oddly, did not change version!
  - (Confirmed that all testing apps now show safe.)
- Eric Throndson @EricThrondson
  - @SGgrc My Nexus 6 is getting MMS messages from random numbers that I assume have #Stagefright. I'm patched, but nervous and annoyed.
- Bob Thibodeau @bobthibincs
  - @SGgrc: got a notice from AT&T to update, no longer vulnerable to Stagefright,

One of the critical Android Stagefright patches was incomplete

- Exodus Intelligence: (CVE-2015-3864) Stagefright: Mission Accomplished?
  - https://blog.exodusintel.com/2015/08/13/stagefright-mission-accomplished/
- Stagefright Patch Incomplete Leaving Android Devices Still Exposed
  - https://threatpost.com/stagefright-patch-incomplete-leaving-android-devices-still-exposed/114267
- Patch Comment: When the sum of the 'size' and 'chunk_size' variables is larger than 2^32, an integer overflow occurs. Using the resulting (overflowed) value to allocate memory leads to an undersized buffer allocation and later a potentially exploitable heap corruption condition. Ensure that integer overflow does not occur.
- Patch for CVE-2015-3824, aka Google Stagefright 'tx3g' MP4 Atom Integer Overflow, was quite simple, consisting of 3 lines of added code:

```
+               if (SIZE_MAX - chunk_size <= size) {
+               return ERROR_MALFORMED;
+               }
```

  - *SIZE_MAX* (*0xFFFFFFFF*)
  - *size* is of *size_t* type which is an *unsigned int*.
  - type of *chunk_size*, is *uint64_t*.
  - "chunk_size" is 64 bits, and 64 bits is loaded from the MP4 metadata, but when storage space is allocated, only the lower 32-bits of the sum are used.
- Exodus argued that it was Google's fault for missing this, and that since they had already used up 120 days since they were informed of the bugs, they were not due any grace period on the fact that they screwed up the fix for one of the problems.
- Zimperium's StageFright Detector IS updated with awareness of this latest problem.

Android "Google Admin" Sandbox Bypass

- A malicious application on the same device as the Google Admin application is able to read

data from any file within the Google Admin sandbox, bypassing the Android Sandbox.

- "Google Admin (by Google) lets you manage your Google for Work account on-the-go. Add and manage users and groups, contact support, and view audit logs for your organization.

  FOR WHOM? - This app is only for super administrators of Google for Work products, including Google Apps for Work, Education, Government, Google Coordinate, and Chromebooks.

  It provides the following features:

  • User Management Features - Add/Edit user, Suspend user, Restore user, Delete user, Reset password

  • Group Management Features - Add/Edit Group, Add members, Delete group, View group members
- March: Google notified and acknowledged problem.
- May: MWR asks how it's going, Google asks for 2 more weeks to get the patch out.
- June: MWR requests another update. Google acknowledges they have exceeded their own 90-day disclosure deadline… asks for disclosure delay until July.
- August: After five months with no results, MWR informs Google of intent to disclose.

Windows 10… can't stop talking to Microsoft

- Even when told not to, Windows 10 doesn't stop talking to Microsoft
- It's no wonder that privacy activists are up in arms.
  - http://arstechnica.co.uk/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft/
- Windows 10 sends data to Microsoft, despite privacy settings
- Some of the information sent back to Microsoft can identify the user's machine.
  - http://www.zdnet.com/article/windows-10-sends-data-to-microsoft-despite-privacy-settings/
- ArsTechnica observes and reports:
  - With Cortana and searching the Web from the Start menu disabled, opening Start and typing will send a request to www.bing.com to request a file called threshold.appcache which appears to contain Cortana information, even though Cortana is disabled. And the request for this file appears to contain a persistent machine identifier that persists across reboots.
  - Not a big deal, but… Some of the traffic looks harmless but feels like it shouldn't be happening. For example, even with no Live tiles pinned to Start (and hence no obvious need to poll for new tile data), Windows 10 downloads new tile info from MSN's network from time to time, using unencrypted HTTP to do so. While the requests contain no identifying information, it's not clear why they're occurring at all, given that they have no corresponding tile.
  - Other traffic looks a little more troublesome. Windows 10 periodically sends data to a Microsoft server named ssw.live.com. This server seems to be used for OneDrive and some other Microsoft services. Windows 10 transmits information to the server even when OneDrive is disabled and logins are using a local account that isn't connected to a Microsoft Account. The exact nature of the information being sent isn't clear—it appears to be referencing telemetry settings—and again, it's not clear why any data is being sent at all since telemetry was disabled using group policies.
- Windows 10 is a deeply cloud-connected OS...

(Win10 Privacy Reality Check:)

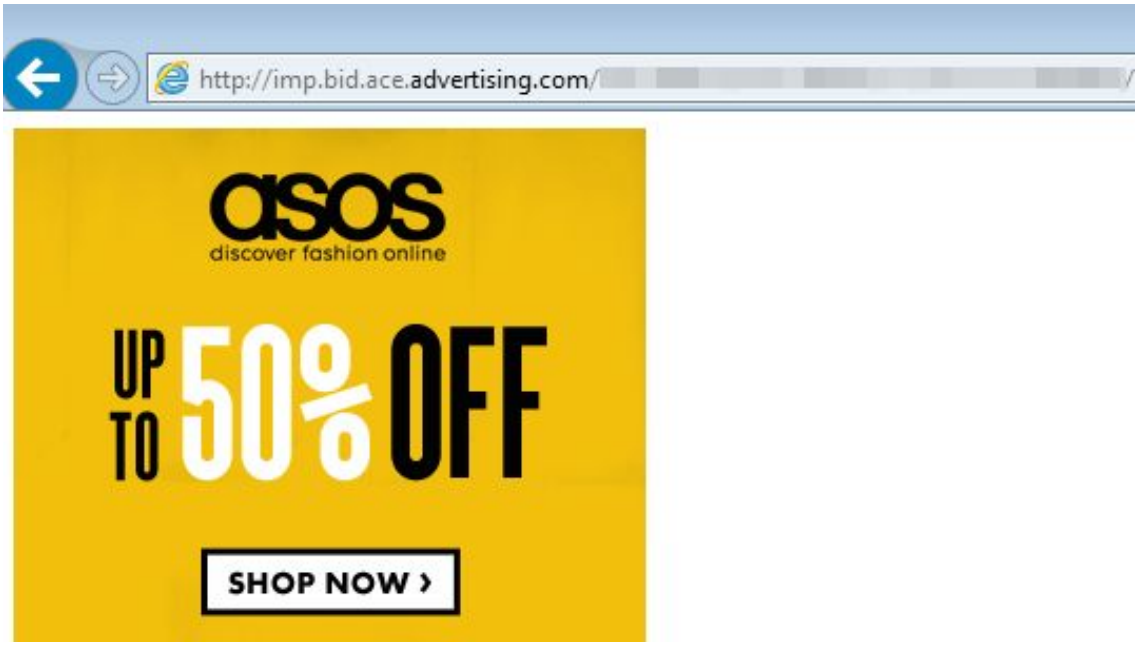
- Simon Zerafa @SimonZerafa RT Fenrir @semibogan
  "Windows 10 is a privacy nightmare!", they said on twitter, while using Google, and updating Facebook.

Malvertising continues to expand

- June and July have set new records for malvertising attacks.
- Yahoo! pages, at 6.9 billion visits/month, were serving malware.
  - Yahoo! was notified and responded immediately.
- A chain of JavaScript, successively loaded by each retrieval and then executed...
- **ads.yahoo.com**
  -> adslides.rotator.hadj1.adjuggler.net
  -> ch2-34-ia.azurewebsites.net/?ekrug=sewr487giviv93=12dvr4g4
  -> basestyle.org/?id=1423150231&JHRufu346&camp=URhfn67458&click=UEjd856
  -> siege.nohzuespoluprace.net/forums/viewforum.php?f=2sb49&sid=y1yki0
- The sequence of redirections eventually leads to the Angler Exploit Ki.
- Angler has been dropping a mix of ad fraud (Bedep) and ransomware (CryptoWall).

- MalwareBytes Blog writes:
  Malvertising is a silent killer because malicious ads do not require any type of user interaction in order to execute their payload. The mere fact of browsing to a website that has adverts (and most sites, if not all, do) is enough to start the infection chain.
  The complexity of the online advertising economy makes it easy for malicious actors to abuse the system and get away with it. It is one of the reasons why we need to work very closely with different industry partners to detect suspicious patterns and react very quickly to halt rogue campaigns.

- MalwareBytes updates on this malvertising campaign they've been monitoring:
  - August 14th: Campaign moves to a new advertiser (AOL) and an Azure domain...



- Utilizes a series of chained, JavaScript-driven, SSL-tunnelled fetches:
  - Malvertising URL: imp.bid.ace.**advertising.com**/{redacted}pmcpmprice=0.545/{redacted}dref=http://www.**ebay.com**/sch/i.html?_nkw=jazzy+wheelchair+battery&_pgn=3&_skc=100&rt=nc
  - First Redirection: v5tr34-a09.**azurewebsites.net**/?=a09vv5vtrkp
  - Second Redirection: **mbiscotti.com**/?Xz29TuVbablQc
  - Angler exploit kit:
    - abgzdbergzr.jeppe.iemooentypo.com/{redacted}
    - abgzdbergzr.le9.anguo**anti-malware**.net/abgzdbergzr/{redacted}

- MalwareBytes' telemetry captured this malvertising on **eBay.com**
- Visitors browsers that were served that ad were redirected to the Angler exploit, known for dropping ransomware and ad fraud malware.

HuffingtonPost Malvertising - for the fourth time since December 2014

- http://www.cyphort.com/100m-huffington/
- HuffingtonPost, news website visited by over 100 million people monthly (ComScore Media Metrix).
- On Aug 13, Cyphort Labs identified a malvertising infection seen redirecting visitors to a malicious exploit kit.
- Cyphort Labs has previously detected and reported on HuffingtonPost malvertising on:
  - December 31, 2014 – HuffingtonPost installs Kovter Trojan via Neutrino exploit kit
  - February 3, 2015 – LAWeekly, HuffingtonPost hit by AOL Ad-network malvertising
  - July 16, 2015 – Malvertising uses SSL redirectors
- Chain:
  - finish class.choozpildyk.com/civis/viewforum.php?<malware>
  - redirect arqadrgbdd.wpara.feeyunippon1.net
  - redirect arqadrgbdd.porsc.thahtparsianinsurance.net
  - https mbiscotti.com
  - https v5tr34-a09.azurewebsites.net
  - https secserv.adtech.de
  - redirect imp.bid.ace.advertising.com
  - redirect uac.advertising.com
  - redirect leadback.advertising.com
  - redirect an.tacoda.net
  - redirect cdn.at.atwola.com
  - redirect o.aolcdn.com
  - start huffingtonpost.com

- Advertising.com (part of AOL Platforms) was the culprit again. It has 199 million unique visitors per month, and reaches 88.8% of the US internet audience. We have reached out to AOL security team and reported this issue.
- The cyber criminals are always looking for mass distribution of their payloads and they get their wish fulfilled with malvertising. It is much easier to infect a popular site via its Ads provider and reach millions of people, than to try to put malware on the individual victim's computers. We expect high-profile malvertising cases to continue.

Kaspersky Antivirus accused of creating fake malware for over 10 years

- Exclusive: Russian antivirus firm faked malware to harm rivals - Ex-employees
  - http://www.reuters.com/article/2015/08/14/us-kaspersky-rivals-idUSKCN0QJ1CR20150814
- http://thenextweb.com/insider/2015/08/14/kaspersky-antivirus-accused-of-creating-malware-for-over-10-years/
- According to two former employees: Starting more than a decade ago, one of the largest security companies in the world, Moscow-based Kaspersky Lab, tried to damage rivals in the marketplace by tricking their rivals' antivirus software programs into classifying benign files as malicious.
- They said the secret campaign targeted Microsoft, AVG, Avast, and other rivals, fooling some of them into deleting or disabling important files on their customers' PCs.
- They said some of the attacks were ordered by Kaspersky Lab's co-founder, Eugene Kaspersky, in part to retaliate against smaller rivals who he felt were copying his software instead of developing their own technology.
- One of the former employees said "Eugene considered this stealing." Both sources requested anonymity and said they were among a small group of people who knew about the operation.
- Kaspersky Lab strongly denied that it had tricked competitors into categorizing clean files as malicious, so-called false positives.

- Microsoft, AVG and Avast **had** previously reported to Reuters that unknown parties had tried to induce false positives in recent years. When contacted this week, they had no comment on the allegation that Kaspersky Lab had targeted them.
- In recent years, as the problem of rapid malware detection has grown, so has collaboration.
- In an effort to prove that other companies were ripping off its work, Kaspersky said it ran an experiment: It created 10 harmless files and told VirusTotal that it regarded them as malicious. VirusTotal aggregates information on suspicious files and shares them with security companies.
- Within a week and a half, all 10 files were declared dangerous by as many as 14 security companies that had blindly followed Kaspersky's lead, according to a media presentation given by senior Kaspersky analyst Magnus Kalkuhl in Moscow in January 2010.
- When Kaspersky's complaints did not lead to significant change, the former employees said, it stepped up the sabotage.
- In one technique, Kaspersky's engineers would take an important piece of software commonly found in PCs and inject bad code into it so that the file looked like it was infected, the ex-employees said. They would send the doctored file anonymously to VirusTotal.
- Then, when competitors ran this doctored file through their virus detection engines, the file would be flagged as potentially malicious. If the doctored file looked close enough to the original, Kaspersky could fool rival companies into thinking the clean file was problematic as well … thus creating active false-positives in the field and harming competitors.

- Eugene Kaspersky @e_kaspersky - 7:56 AM - 14 Aug 2015
  - I don't usually read @reuters. But when I do, I see false positives.
    For the record: this story is a complete BS: https://kas.pr/1eka

Lenovo's new Dirty Tricks

- After Superfish…
- Pre-Boot BIOS code replaces Windows files.
  - ArsTechnica Forum: http://arstechnica.com/civis/viewtopic.php?p=29497693&sid=ddf3e32512932172454de515091db014#p29497693
- If Windows 7 or 8 is installed, the BIOS of the laptop checks 'C:\Windows\system32\autochk.exe' to see if it's a Microsoft file or a Lenovo-signed one, then overwrites the file with its own.
- Then, when the modified autochk file is executed on boot, another two files LenovoUpdate.exe and LenovoCheck.exe are created, which set up a service and download files when connected to the internet.

- "Absolute CompuTrace"
  - https://www.blackhat.com/docs/us-14/materials/us-14-Kamluk-Computrace-Backdoor-Revisited-WP.pdf
  - Uses BIOS-time pre-boot to reach into the file system to replace "autochk.exe" with their own code, which Windows executes early in the boot process.
  - Installs a powerful RAT - Remote Access Trojan

- Windows Platform Binary Table (WPBT) - Introduced in 2011 (Win8) & updated July 2015.
  - http://download.microsoft.com/download/8/A/2/8A2FB72D-9B96-4E2D-A559-4A27CF905A80/windows-platform-binary-table.docx
  - ***Abstract:*** A platform can be provisioned with the Windows operating system by entities including an enterprise, a system reseller, or an end-user customer. If the platform has drivers, system services, or executable files that are integral to the platform, the platform binaries must either be distributed as part of the Windows image or they must be injected into the Windows image by each of the possible provisioning entities. A rich set of tools exist to aid Windows provisioning, ranging from driver injection and offline registry management to sysprep imaging tools. However, there is a small set of software where the tools are not enough. The software is absolutely critical for the execution of Windows, but for one reason or another, the vendor is unable to distribute the software to every provisioning entity.
    This paper describes a mechanism for a platform, via the boot firmware, to publish a binary to Windows for execution. The mechanism leverages a boot firmware component to publish a binary in physical memory described to Windows using a fixed ACPI table.
  - NOTE: The on-disk file location is \Windows\System32\Wpbbin.exe on the operating system volume.

For BlackHat, Fireeye analyzes the current state of Android fingerprint security

- https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf
- On the HTC One Max X the fingerprint is saved as /data/dbgraw.bmp with a 0666 permission setting (world readable). Any unprivileged processes or apps can steal user's fingerprints by reading this file. This was a mistake and was quickly corrected by HTC.
- Even if the protection of fingerprint data in TrustZone is trustworthy, it only means that

the fingerprints previously registered on the devices are secured. Fireeye found that the fingerprint sensor itself in many devices is still exposed to the attackers. Although the ARM architecture enables isolating critical peripherals from being accessed outside TrustZone (by programming the TrustZone Protection Controller), most vendors fail to utilize this feature to protect fingerprint sensors.
- As of writing, we have confirmed this vulnerability on HTC One Max, Samsung Galaxy S5, and others. All vendors have provided patches after Fireeye's notification.

AT&T Helped U.S. Spy on Internet on a Vast Scale

- http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html
- Newly disclosed [Edward Snowden] N.S.A. documents show that the relationship with AT&T has been considered unique and especially productive. One document described it as "highly collaborative," while another lauded the company's "extreme willingness to help."
- AT&T's cooperation has involved a broad range of classified activities, according to the documents, which date from 2003 to 2013. AT&T has given the N.S.A. access, through several methods covered under different legal rules, to billions of emails as they have flowed across its domestic networks.
- AT&T provided technical assistance in carrying out a secret court order permitting the wiretapping of all Internet communications at the United Nations headquarters, a customer of AT&T.
- AT&T installed surveillance equipment in at least 17 of its Internet hubs on American soil, far more than its similarly sized competitor, Verizon. And its engineers were the first to try out new surveillance technologies invented by the eavesdropping agency.
- One document reminds N.S.A. officials to be polite when visiting AT&T facilities, noting, "This is a partnership, not a contractual relationship."
- The NYTimes story is long and covers many more specific program names and deep history.

Wuala shutting down, recommending Tesorit

- https://support.wuala.com/2015/08/wuala-shutdown-notice/
- Yesterday, 17 Aug 2015: No further renewals or purchase of storage
- Sept 30, 2015: Wuala service will transition to read-only
- Nov 15, 2015: Wuala service terminates, all data stored in the Wuala cloud will be deleted
- Please download the content in your Wuala account and safely backup it to your PC, Mac, external hard drive or another cloud storage provider. After *15 November 2015,* you will no longer have access to your content, which will be deleted. Please use this time to download and backup the content stored in your Wuala account.
- Wuala suggests switching to Tresorit (Swiss-Hungarian)
    - https://tresorit.com/business/wuala-alternative

Miscellany:

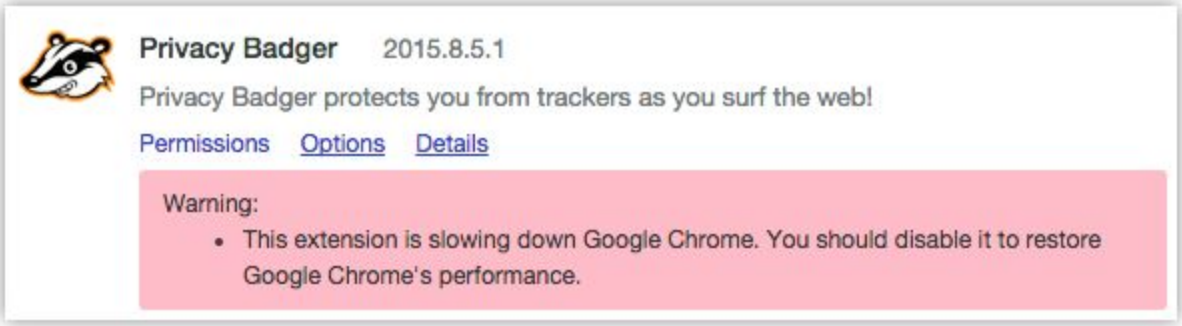
The Quest for Surfing Safety:

- CubeOS, etc.
- Trouble with a VM... Links in and downloads out
- Sandboxie

Privacy Badger vs Google & Chrome?

- Jason Fiore @yuusharo
  - I've used Chrome for 7 years. I've NEVER seen this message until this today. Google doesn't like @EFF... (cc @SGgrc) pic.twitter.com/QVpVS4L3hB
  - http://t.co/QVpVS4L3hB

Hmm… Chrome's not a big fan of Privacy Badger. Imagine that!



SpinRite:

Chris in Atlanta
Subject: SpinRite and drive quality over the years
Date: 10 Aug 2015 14:00:47
:
Hey Steve and Leo,

Love the show blah, blah
A quick spinrite story for you.

I was recently moving and getting ready to clean out the backlog of old drives I had in drawers and boxes.

I started running SpinRite and DBAN on the drives repairing and wiping each.

Going through the box, I found one of the first drives I ever owned, a 40Mb IDE drive off my first 486DX.

This is a drive that has sat in the bottom of a dusty box for almost 20+ years without a static

bag, going through 5+ moves across the country, and years in houses without air conditioning. I wondered whether it would even spin.

It was immaculate!

You often talk about the degree to which drive manufacturers have stretched and crammed every last bit they could onto each platter, and stretched error correction to, or sometimes past, the limit. I have seen no better example of the tangible implications of this than seeing such a reminder of how solid old drives actually were.

Just thought I'd share the story and the love for spinrite.

Three Interesting Takes on Today's Internet Advertising

"The ethics of modern web ad-blocking"

- I'm Marco Arment: a programmer, writer, podcaster, geek, and coffee enthusiast.
- http://www.marco.org/2015/08/11/ad-blocking-ethics
- http://bit.ly/sn-521
- <Opening quote> More than fifteen years ago, in response to decreasing ad rates and banner blindness, web advertisers and publishers adopted pop-up ads.

"Safari Content Blocker, Before and After"

- July 8th: John Gruber, Daring Fireball
- http://daringfireball.net/2015/07/safari_content_blocker_imore
- Dean Murphy wrote an iOS 9 Safari Content Blocker, and tested it against iMore:

  With no content blocked, there are 38 third party scripts (scripts not hosted on the host domain) running when the homepage is opened, which takes a total of 11 seconds. Some of these scripts are hosted by companies I know, Google, Amazon, Twitter and lots from companies I don't know. Most of which I assume are used to display adverts or track my activity, as the network activity was still active after a minute of leaving the page dormant. I decided to turn them all off all third party scripts and see what would happen.

  After turning off all third party scripts, the homepage took 2 seconds to load, down from 11 seconds. Also, the network activity stopped as soon as the page loaded so it should be less strain on the battery.

  I love iMore. I think they're the best staff covering Apple today, and their content is great. But count me in with Nick Heer — their website is shit-ass. Rene Ritchie's response acknowledges the problem, but a web page like that — Rene's 537-word all-text response — should not weigh 14 MB.1

  It's not just the download size, long initial page load time, and the ads that cover valuable screen real estate as fixed elements. The fact that these JavaScript trackers hit the network for a full-minute after the page has completely loaded is downright criminal. Advertising should have minimal effect on page load times and device battery life.

  Advertising should be respectful of the user's time, attention, and battery life. The

industry has gluttonously gone the other way. iMore is not the exception — they're the norm. 10+ MB page sizes, minute-long network access, third-party networks tracking you across unrelated websites — those things are all par for the course today, even when serving pages to mobile devices. Even on a site like iMore, staffed by good people who truly have deep respect for their readers.

With Safari Content Blockers, Apple is poised to allow users to fight back. Apple has zeroed in on what we need: not a way to block ads per se, but a way to block obnoxious JavaScript code. A reckoning is coming.

Content blockers, bad ads, and what we're doing about it

- July 9th: Rene Ritchie: http://www.imore.com/content-blockers-bad-ads-and-what-were-doing-about-it
- Strongest message was that, much as they would really wish to… today's ad ecosystem provides them with effectively zero control.
- The either advertise or die… and no one wants iMore to die.
- … so even the best people have their hands tied.