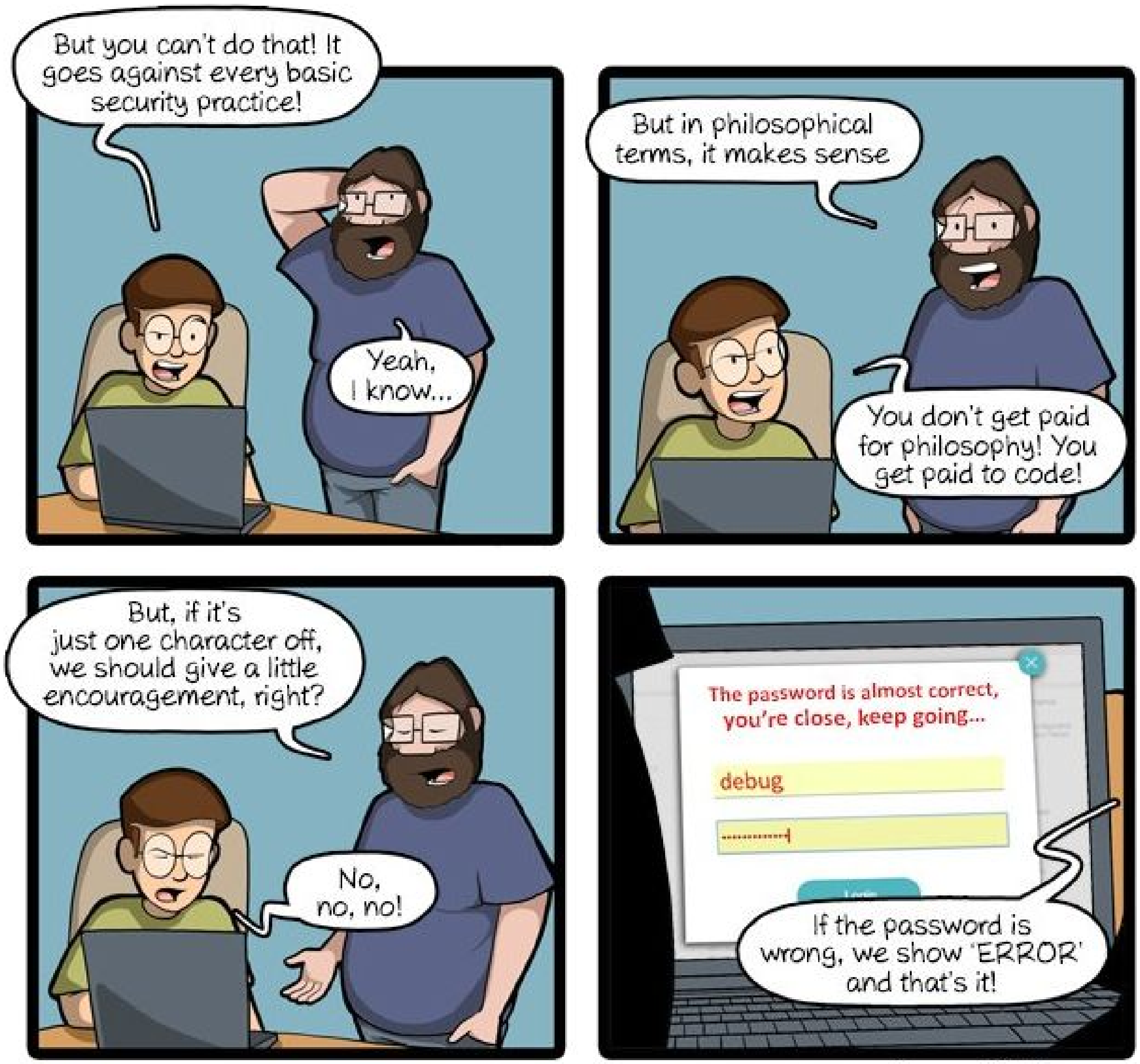
Security Now! #647 - 01-23-18

Dark Caracal

This week on Security Now!

The Meltdown and Spectre vulnerabilities continue to dominate the week's news. So we'll first catch up with what's new there, then discuss the new Net Neutrality violation detection apps that are starting to appear, a new app and browser plug from the search privacy provider DuckDuckGo, a bit of welcome news from Apple's Tim Cook about their planned response to the iPhone battery-life and performance debacle, a bit of errata and some feedback from our terrific listeners. Then we take a look into a state-level, state-sponsored, worldwide, decade-long cyber espionage campaign which the EFF and Lookout Security have dubbed: Dark Caracal.

Our Picture of the Week


But you can't do that! It goes against every basic security practice!
Yeah, I know...
But in philosophical terms, it makes sense
You don't get paid for philosophy! You get paid to code!
But, if it's just one character off, we should give a little encouragement, right?
No, no, no!
The password is almost correct, you're close, keep going...
debug
If the password is wrong, we show 'ERROR' and that's it!

CommitStrip.com

Security News

Intel Firmware Update Reboot Issues:
Monday, Jan 22nd: "Root Cause of Reboot Issue Identified; Updated Guidance for Customers and Partners"
https://newsroom.intel.com/news/root-cause-of-reboot-issue-identified-updated-guidance-for-customers-and-partners/

From Intel's "NewsRoom"...
"As we start the week, I want to provide an update on the reboot issues we reported Jan. 11. We have now identified the root cause for Broadwell and Haswell platforms, and made good progress in developing a solution to address it. Over the weekend, we began rolling out an early version of the updated solution to industry partners for testing, and we will make a final release available once that testing has been completed.

Based on this, we are updating our guidance for customers and partners:

We recommend that OEMs, cloud service providers, system manufacturers, software vendors and end users stop deployment of current versions, as they may introduce higher than expected reboots and other unpredictable system behavior. For the full list of platforms, see the Intel.com Security Center site."

Meanwhie, the technical side says...
"Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method"
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

Updated Jan. 22

We have now identified the root cause of the reboot issue impacting Broadwell and Haswell platforms, and made good progress in developing a solution to address it. Based on this, we are updating our guidance for customers and partners:

We recommend that OEMs, Cloud service providers, system manufacturers, software vendors and end users stop deployment of current versions on the below platforms, as they may introduce higher than expected reboots and other unpredictable system behavior.

We also ask that our industry partners focus efforts on testing early versions of the updated solution for Broadwell and Haswell we started rolling out this weekend, so we can accelerate its release. We expect to share more details on timing later this week.

For those concerned about system stability while we finalize the updated solutions, we are also working with our OEM partners on the option to utilize a previous version of microcode that does not display these issues, but removes the Variant 2 (Spectre) mitigations. This would be delivered via a BIOS update, and would not impact mitigations for Variant 1 (Spectre) and Variant 3 (Meltdown).

We believe it is important for OEMs and our customers to follow this guidance for all of the specified platforms listed below, as they may demonstrate higher than expected reboots and unpredictable system behavior. The progress we have made in identifying a root cause for Haswell and Broadwell will help us address issues on other platforms. Please be assured we are working quickly to address these issues.

- The guidance applies to at least some of the processors from Intel's last several generations of chips, with affected models in the Broadwell, Haswell, Coffee Lake, Kaby Lake, Skylake, and Ivy Bridge families.

- Certain lines are affected more than others. For example, only Ivy Bridge datacenter/workstation processors are included. But chips from most recent consumer lines also appear to be impacted.

- Intel says that it's identified the issue behind the unexpected reboots on Broadwell and Haswell processors and is working toward releasing an update that addresses the exploits without causing that issue.

- But the same problems have been seen on Ivy Bridge, Sandy Bridge, Skylake, and Kaby Lake processors too.

- Intel says it's "actively working on developing solutions" for those platforms as well.

Meanwhile, Linus Torvalds has been having a temper tantrum meltdown (so to speak) over Intel's apparent plans.
https://lkml.org/lkml/2018/1/21/192
Linus' expletive-filled tirade appears to be complaining about Intel's short and medium-term plans to deal with the Spectre mitigations.

This appears to boil down to the fact that Linus isn't happy with the "disable all branch prediction" mitigation which, for the time being, is really all that Intel can do.

(Let's talk about the limitations of Microcode…)

Woody on Windows for ComputerWorld has patch updates:
https://www.computerworld.com/article/3249767/microsoft-windows/patching-meltdown-windows-fixes-sloppy-net-warnings-about-word-and-outlook.html

2018-01 Cumulative Update for Windows 10 Version 1709 for x86-based Systems (KB4073291)

Win10 Fall Creators Update version 1709 — Cumulative update KB 4073291 brings the Meltdown/Spectre patches to 32-bit machines. What, you thought 32-bit machines already had Meltdown/Spectre patches? Silly mortal. Microsoft's Security Advisory ADV180002 has the dirty details in the fine print, point 7:

Q: I have an x86 architecture and the PowerShell Verification output indicates that I am not fully protected from these speculative execution side-channel vulnerabilities. Will Microsoft provide complete protections in the future?

A: Addressing a hardware vulnerability with a software update presents significant challenges and mitigations for older operating systems that require extensive architectural changes. The existing 32 bit update packages listed in this advisory fully address CVE-2017-5753 and CVE-2017-5715, but do not provide protections for CVE-2017-5754 at this time. Microsoft is continuing to work with affected chip manufacturers and investigate the best way to provide mitigations for x86 customers, which may be provided in a future update.

It appears as if this is the first 32-bit version of Windows that has a patch for the Meltdown vulnerability. Surprise.

Like most of the patches I talked about yesterday, this one is available only through the Update Catalog — it won’t be pushed onto your machine.

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4073291

"Defend Net Neutrality: Test your Internet"
http://www.testyourinter.net/
OONI (the Open Observatory of Network Interference) has an open source, non-profit app for tracking Internet censorship.

Good news and bad news → False positives, streaming vs bulk download, etc.

Duck Duck Go has a cross-platform privacy-enhancing plugin.
https://spreadprivacy.com/privacy-simplified/

DuckDuckGo the well-known privacy-protecting search provider is now offering a browser plugin.

In their announcement they say: "Today we’re taking a major step to simplify online privacy with the launch of fully revamped versions of our browser extension and mobile app, now with built-in tracker network blocking, smarter encryption, and, of course, private search – all designed to operate seamlessly together while you search and browse the web. Our updated app and extension are now available across all major platforms – Firefox, Safari, Chrome, iOS, and Android – so that you can easily get all the privacy essentials you need on any device with just one download."

Tim Cook Promises to Let iPhone Users Turn Off Throttling Soon
https://gizmodo.com/tim-cook-promises-to-let-iphone-users-turn-off-throttli-1822188874

Errata

- **Sean Spratt @seanspratt**
  @SGgrc on your podcast you said only post-Haswell has INVPCID support. However, I'm reading elsewhere that INVPCID is include in Haswell? InSpectre says I have high-performance Meltdown protection. So, yes, I have INVPCID?

- **Richard Tan @richard_tan**
  Hi hope you are well. I keep hearing on security now that haswell and down would not be patch with the performance fix, but Haswell seems to be the first set of processor that has INVPCID. So should it be that Haswell onwards should get the performance fix for meltdown?

Process Context ID (PCID) was introduced by Intel's Westmere architecture January 7, 2010.

Invalidate PCID (INVPCID) with Haswell
Haswell is the codename for the processor microarchitecture developed by Intel as the "fourth-generation core" successor to the Ivy Bridge microarchitecture. Intel officially announced CPUs based on this microarchitecture on June 4, 2013.

SpinRite

anisotropic / @denshangyinyang
@SGgrc todays update (SpinRite 6 on window 10 64bit) OK after a gruelling 17 hour at level 3 (on normal non problematic hard drive (1 terabyte) I can safely say this product is awesome! from what I could notice? It fixed all oddities in, but also out of windows, BIOS resolution! ty

Closing The Loop

S Wayne Martin @SWayneMartin
@SGgrc Hey, can you comment on how you determine performance when your InSpectre says performance is "Good". Seems that would require a benchmark to determine. Curious minds.

Alessandro Canepa @canepa
@SGgrc #WebMon (cmcode.co.uk/webmon/) doesn't seem monitor HTTPS websites.
Do you know of any alternatives? #SecuirtyNow #TwitTV #SpinRite??

Guillermo García @gmogarciag
@SGgrc #SN644 how do you “baby” your iPhone’s battery??

Darrel McQuienn @mithrilrat
With respect to precision time. It’s quite important in a lot of applications.
I do traffic control systems and astronomy. Both of which require precision time.

markzip @markzip
@SGgrc You say that DV certificates are free and easy so http should/will die. But what about those of us on shared servers in hosting providers who are *not offering Let's Encrypt? These large providers have no plans to do so because it cuts in to their charging for certs.

Dark Caracal

The authors explain: “In keeping with traditional APT naming, we chose the name “Caracal” (pronounced [kar-uh-kal]) because the feline is native to Lebanon and because this group has remained hidden for so long. From the Wikipedia entry “the caracal is highly secretive and difficult to observe” and “is often confused with [other breeds of cat].”

Dark Caracal Technical Report: https://www.lookout.com/info/ds-dark-caracal-ty

https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

EFF and Lookout Uncover New Malware Espionage Campaign Infecting Thousands Around the World
https://www.eff.org/press/releases/eff-and-lookout-uncover-new-malware-espionage-campaign-infecting-thousands-around

This is a global cyber-espionage campaign being managed and run from the building of the General Directorate of General Security (GDGS) in Beirut, Lebanon.

The GDGS is known to gather intelligence for national security purposes and for its offensive cyber capabilities.

Dark Caracal is reusing the same infrastructure -- command and control servers, IP addresses, hosting and database providers, domain registrars, etc. -- as was previously seen in the Operation Manul campaign, which targeted journalists,
lawyers, and dissidents critical of the government of Kazakhstan.

The Dark Caracal effort has been conducting a multi-platform, Advanced Persistence Threat (APT)-level surveillance operation targeting individuals and institutions globally.

Hundreds of gigabytes of data has been identified as having been exfiltrated from thousands of victims, spanning 21+ countries in North America, Europe, the Middle East, and Asia.

The mobile component of this APT is one of the first we've seen executing espionage on a global scale.

Analysis shows Dark Caracal successfully compromised the devices of military personnel, enterprises, medical professionals, activists, journalists, lawyers, and educational institutions. Dark Caracal targets also include governments, militaries,
utilities, financial institutions, manufacturing companies, and defense contractors.

Types of exfiltrated data include documents, call records, audio recordings, secure messaging client content, contact information, text messages, photos, and account data.

Dark Caracal follows the typical attack chain for cyber-espionage, relying primarily upon social media, phishing, and in some cases physical access to compromise target systems, devices, and accounts.

Some of Dark Caracal's espionage technology appears to have been developed in house -- and is shared among various campaigns -- and other technology is purchased from or borrowed from the dark web.

Lookout first discovered the presence of "Pallas" -- an implant used in multiple Trojanized Android applications -- in May 2017.

Dark Caracal also makes extensive use of a Windows malware known as Bandook RAT (RAT = Remote Access Trojan). And Dark Caracal also uses a previously unknown multi-platform (Windows/OSX/Linux) tool, written in JAVA, which Lookout and the EFF have dubbed: CrossRAT.

Dark Caracal employs a continuously evolving global network infrastructure. The infrastructure operators prefer to use Windows and the XAMPP stack on their C2 servers rather than the traditional LAMP stack.

With this report, Lookout and the EFF are releasing more than 90 indicators of compromise (IOC):

- 11 Android malware IOCs
- 26 desktop malware IOCs
- 60 domains, IP Addresses, and WHOIS information

The paper details: WiFi networks and SSIDs, IP addresses, the hosting providers being used, the pseudonyms under which various services have been registered.

There are fully mature watering hole servers and phishing domains closely mimicking Facebook and Twitter websites... and mature phishing attack campaigns aimed to lure targeted victims to the phony spoofed sites.

Dark Caracal relies primarily on social engineering via posts on a Facebook group and WhatsApp messages in order to compromise target systems, devices, and accounts. At a high-level, the attackers have designed three different kinds of phishing messages, the goal of which is to eventually drive victims to a watering hole controlled by Dark Caracal.

Surveillanceware — Mobile Capabilities Pallas — Dark Caracal’s Custom Android Samples

Using their global sensor network, Lookout researchers were able to identify 11 unique Android surveillanceware apps. The trojanized apps retain the legitimate functionality of the apps they spoof and behave as intended.

The apps are found predominantly in trojanized versions of well-known secure messaging apps including:

- Signal (org.thoughtcrime.securesms)
- Threema (ch.threema.app)
- Primo (com.primo.mobile.android.app)
- WhatsApp (com.gbwhatsapp)
- Plus Messenger (org.telegram.plus)

Neither the desktop nor the mobile malware tooling use zero day vulnerabilities. They are simply downloaded instead of the intended application and then rely upon the permissions granted at installation to access sensitive user data.

However, there are functions to allow an attacker to instruct an infected device to download and install additional applications or updates. This means it’s possible for the operators behind Pallas to push specific exploit modules to compromised devices to gain additional complete access.

Desktop Screenshots - This data included full screenshots taken at regular intervals and uploaded to adobeair[.]net.

The authors of this report write: By observing these images, it is disturbingly simple to watch a victim go about his daily life and follow that individual every step of the way.

Quote: "Not only was Dark Caracal able to cast its net wide, it was also able to gain deep insight into each of the victim’s lives. It did this through a series of multi-platform surveillance campaigns that began with desktop attacks and pivoted to the mobile device. Stolen data was found to include personal messages and photos as well as corporate and legal documentation. In some cases, screenshots from its Windows malware painted a picture of how a particular individual spent his evenings at home.