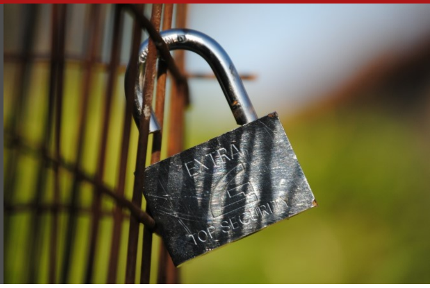
IN THIS ISSUE >>> #39

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

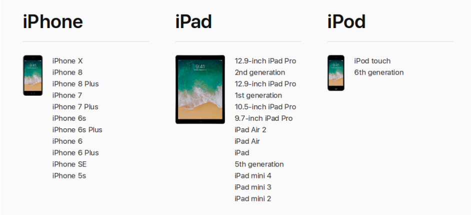
Digital Update



iOS 11/11.0.1

The Good, The Bad, The WTF

If you are an iPhone user, by now you should have received the iOS 11 update that was pushed out on September 21st to millions of iPhones across the world (list of devices below). This was a highly anticipated update and unfortunately, there are quite a few bugs and issues with iOS 11 at this time. The good news is just like all of the previous updates, Apple will eventually fix all of the issues and push out a patch. They have already pushed out a patch in the form of 11.0.1, but the new iOS is still quite unstable. If you haven't updated your iPhone yet, you may wish to wait a few weeks before doing so and hopefully by then it will be stable enough to regularly use. We are not saying not to update, we are just saying iOS 11 is not quite stable and you may want to postpone the update. Right off the bat, after the update, your Bluetooth is automatically turned back on for you just like every other major update in the past. Be sure to turn that off as we've talked about the dangers of Bluetooth in the past. If you swipe up from the bottom of the screen, you will see the new and improved control center which is not as customizable as they will have you believe. You have a few apps that can be added to the bottom of the control center, but you can't add things like Location Services, which is something we were hoping to see. You can toggle Wi-Fi, Bluetooth, Cellular, Airdrop, and Airplane mode, but beware: <u>toggling Wi-Fi, Bluetooth or Cellular does not turn off the interfaces, it simply drops the current connection</u>. You still need to go into settings to turn these off completely, although Airplane mode works just fine in the control center to turn the interfaces off. Hopefully Apple fixes this, but we expect it is serving its intended purpose.



iPhone	iPad	iPod
iPhone X iPhone 8 iPhone 8 Plus iPhone 7 iPhone 7 Plus iPhone 6s iPhone 6s Plus iPhone 6 iPhone 6 Plus iPhone SE iPhone 5s	12.9-inch iPad Pro 2nd generation 12.9-inch iPad Pro 1st generation 10.5-inch iPad Pro 9.7-inch iPad Pro iPad Air 2 iPad Air iPad 5th generation iPad mini 4 iPad mini 3 iPad mini 2	iPod touch 6th generation

Do Not Disturb While Driving is another new feature that detects when you are driving and puts your phone in do not disturb mode just like the name implies. How does it do this? Straight from them, "A Bluetooth connection to a car provides the clearest indication that you are in a vehicle." Sounds simple enough, but what if I keep my Bluetooth off? "If your car does not have Bluetooth, iPhone uses other sources of information such as nearby Wi-Fi networks and the accelerometer…" So we are probably going to keep that feature off as well as Bluetooth and Wi-Fi when not in use. **<u>Check back next issue (Oct 15) for more iOS features and recommended settings and practices after the update.</u>**

CURRENT COURSES >>>

- *ESSR*
- *Wireless Analysis*
- *Basic Non-Standard Communications*
- *Advanced Non-Standard Communications*
- *Basic OSINT*
- *Advanced OSINT*
- *Identity Management*
- *NSC RasPi*
- *Data Protection*

CURRENT TOPICS >>>

[Equifax Moves to Fix Weak PINs for "Security Freeze" on Consumer Credit Reports](#)

-Arstechnica

[An Open Letter to the W3C Director, CEO, Team and Membership](#)

-EFF

[CCleaner Command and Control Causes Concerns](#)

-Dark Reading

[Trump Administration Orders Facebook To Hand Over Private Information On 'Anti-Administration Activists'](#)

-Independent

[iOS Just Destroyed Uber's Most Annoying Privacy Flaw](#)

-Slash Gear

[Super Accurate GPS Chips Coming to Smartphones in 2018](#)

-IEEE Spectrum

EVENTS >>>

ToorCamp 2018

June 20-24 2018, San Juan, WA

Black Hat USA 2018

Aug 4-9 2018, Las Vegas, NV

DEF CON 26

Aug 9-12 2018, Las Vegas, NV

READER QUESTIONS >>>

Have a specific **question** you would like us to answer?

Have a suggestion for a **topic**?

Want to **contribute** to the digital update?

Let us know at
digitalupdate@tpidg.us

September's Madness

A lot of things happened in the information security world this month, let's review a few of them.

Equifax Hack

What You Should Know

On July 29th, one of the largest credit bureaus found that someone had unauthorized access to their systems compromising records of over 143 million Americans. There have also been reports of their security standards being sub-par such as their CSO having an art's degree and no experience in security. See our last issue (#38) for the full details of what happened.

What You Should Do

As bad as it sounds, there isn't much you can do other than freeze your credit. Unfortunately the PIN Equifax supplies you is basically a timestamp, so even freezing your credit may not be enough. There are no preventative measures left to take and the only reactive measure is hope you don't get targeted. The good news is you are one in 143 million, so it's highly unlikely you will get targeted first.

CCleaner's 32Bit Swaparoo

What You Should Know

Between August 15th and September 15th, 2.27 Million machines were affected by malware that was placed inside the popular computer cleaning app: CCleaner. Only the 32bit Windows executable (version 5.33.6162) contained the malicious code. The malware extracted basic information from all affected computers. It then sorted through the affected machines and delivered a secondary payload to specific computers. For more information, read the article posted by the [Avast Blog](#).

What You Should Do

This depends on how careful you want to be. The extreme measure would be to factory reset your laptop and rebuild, but you could probably just restore back to a restore point. CCleaner has advised that you update to the latest version and that will fix the problem. This was more of a targeted attack, so there is not much to worry about if you are an average consumer. This attack was aimed at large organizations such as Cisco and the server used to deliver these attacks has since been taken down.

EFF Leaves The W3C

What You Should Know

In a disagreement with the World Wide Web Consortium, the EFF has decided to leave the W3C. The W3C has decided to begin working on something called EME, which is basically an enhancement to DRM. It will allow stricter regulations on copyrights on the internet and allow media companies to say what you can and cannot watch, look at or download. The EFF tried their hardest to get this standard thrown out with no luck. You can read more in their open letter to the W3C [here](#).

What You Should Do

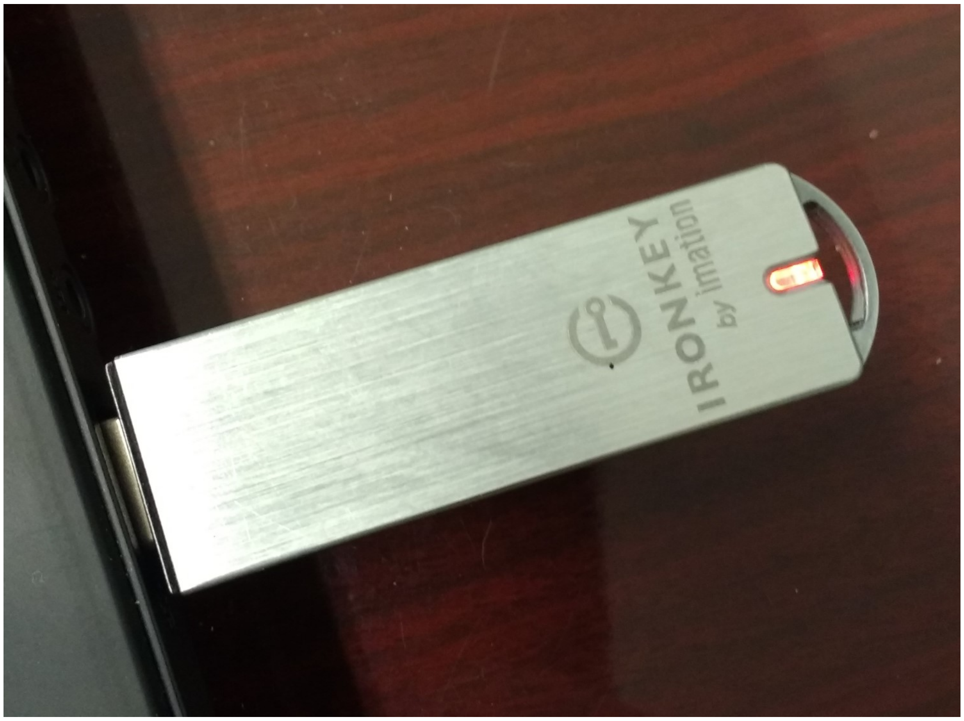
Support a free and open internet. Educate yourself on the associated risks with restricting access to media and giving more power to the already rich and powerful media organizations. A standard like EME is also another attack surface that is only going to get exploited and doesn't help at all with consumer security. Go support the EFF at https://act.eff.org/

BONUS MATERIALS >>>

IronKey's Self Destruction

Don't Try This At Home

Recently, we wanted to waste a lot of money by testing something that no one would ever dare to do purposefully. One because they cost a lot of money and two because if you do what we did with your working device, you will lose everything. We tried out IronKey's self destructing mode to see what happened to the device after the big explosion and to verify that they do actually self-destruct. They make it very difficult to go through all ten attempts by making you unplug and plug the device back at certain intervals. Once we got through all ten attempts, nothing spectacular happened, but when we reinserted the drive, it would not mount. Absolutely nothing showed up when we plugged the IronKey back in and we were greeted with not a green light anymore, but a red one indicating that the IronKey is no longer usable.



So what magic happened to make the once mighty IronKey no longer usable and forever broken? We can't say for certain since IronKey is very much closed source and the only information we have on it is what the developers of the device tell us. They call it "flash-trash technology" and it basically wipes all of the device's flash storage including your encrypted data and the master keys to the encryption. IronKey uses AES-256 to encrypt the storage portion of the device, so even if the data could be recovered, it would take years to brute force the master keys. Pretty handy if you happen to lose your IronKey!

UPDATE CORNER >>>

Software Updates

We preach updates in every class, so here's a list of security software updates for the month of September accompanied by sha256 checksums.

TOR Browser Bundle

Version: 7.0.6

Released: September 28th, 2017

torbrowser-install-7.0.6_en-US.exe

af1b26a2d74b890284e9a2b7826a43bd96d3fe34ba2e54f6b384f3fb226797c8

TorBrowser-7.0.6-osx64_en-US.dmg

4a5b638d2ecc4d7dc4a8708d7d14a1456674ace74a453dc08dc3f3dd4ef47dfb

tor-browser-linux64-7.0.6_en-US.tar.xz

d5e0b7803902d08868bae59de3f939d390c513cc944c9aa28be8dc730ac8e387

TAILS Live ISO

Version: 3.2

Released: September 26th 2017

tails-amd64-3.2.iso

6ead2c7ce076458a31082f1f27444ea94542fe8ee007665e927dfb93c9232a01

Firefox

Version: 56

Released: September 28th, 2017

Firefox Setup 56.0.exe

0448ada5ed1edbe968eb95370e841c7f1a9b5887b258787a531138eaba66adc8

Firefox 56.0.dmg

aae8eb702743ca834b951ae41e14b21f314eef0a67c74e3cd45c459aecdddfdf

firefox-56.0.tar.bz2

eb5938a31076b82ccfebb8c0b6907df582568b39049e982032d227d7ddbc821b

PARTNERS >>>

global communications

FLIR
The World's Sixth Sense

salomon

ROTHCO
COMBAT TESTED SINCE 1953

Silent Pocket

Lenovo

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC
Technical & Tactical Equipment Store

arlo

WD

intel Technology Provider

DELL

CyberPower
Reliability. Quality. Value.

LINKSYS

NETGEAR

cradlepoint

INGRAM MICRO

msi

belkin

Canon

hp

CISCO

PPSS

Nitrokey
secure your digital life

Honeywell
THE POWER OF CONNECTED

redhat

D-Link

vmware

BUFFALO

NVIDIA

KAOS KASPER OSWALD
Ingenieure für innovative Sicherheitslösungen