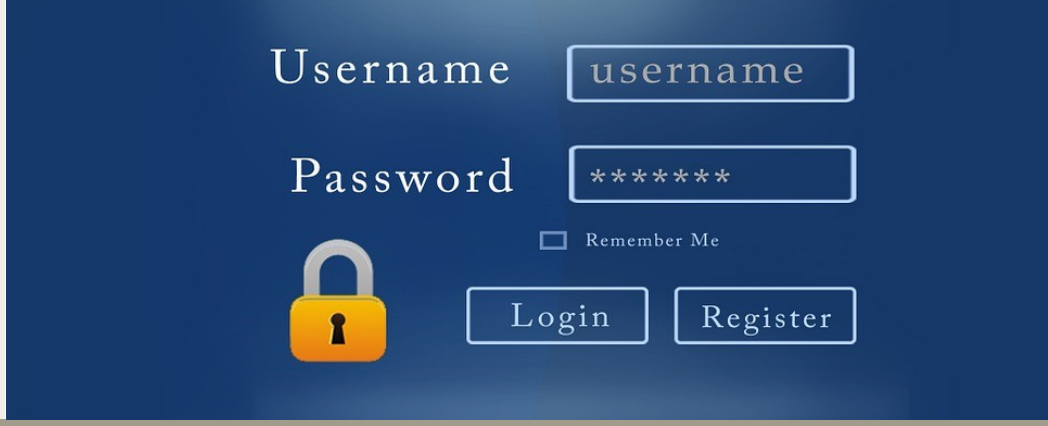
in this issue >>> V.1.15



TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- Apple Tracks Your iMessage Contacts
  - Lifehacker Security
- iOS 10 Bug Makes iTunes Backups More Vulnerable
  - BGR
- Yahoo says 500 Million Accounts Breached by State Actor
  - Ars Technica
- Update Tor and Firefox Immediately—Major Vulnerability Patched
  - Ars Technica
- IoT Devices with Weak Security Used in Massive DDoS Attacks
  - Ars Technica

Signal For Desktop

Private Messaging on the Big Screen

As readers of the update and attendees of our Non-Standard Communications and Digital Protection courses know, Signal is one of the best encrypted messengers on the market. The open-source encryption offers some of the best security currently available. It is so good, its code has been used by WhatsApp and Google's new Allo messenger.

If you're using Signal already—and we hope you are– it just got a lot better. If you're not already using Signal there's a new feature that may change your mind: Signal is now available on your desktop PC, Mac, or Linux computer. Signal's desktop implementation does not yet have a voice capability, but it allows you to send text messages from your computer. These are then synced with your mobile device.

To install the desktop app, you must already have the mobile app and Chrome installed on your computer. Open Chrome, click the icon in the far upper right corner (it looks like three stacked dots). From the drop-down click "Settings". In the settings menu click "Extensions". Scroll all the way to the bottom of the page and click "Get more extensions". Search for "Signal Private Messenger" by Open Whisper Systems.

When the Chrome extension is added it will ask you to open the app on your device. You will then use the app to scan a QR code that will associate the two. Messages between the computer and your mobile will now be synced. We have been using Signal Private Messenger on Mac and Windows platforms since the day it came out, and have no failures to report—it works as advertised.

We like Signal for desktop because it is very convenient. However, there is no username or password required to access your Signal messages, either on desktop or mobile. Because of this you should protect your computer with full disk encryption and your mobile with a long, strong passcode. This ensures that anyone getting their hands on your machine when it is powered off will not be able to see your Signal messages and everything else on the machine. This would bypass the excellent encryption that has gone into the app.

set the stage >>>

Email Masking: 33Mail.com

If you have attended our Non-Standard Communications or Digital Protection Courses, you know that we are big proponents of email masking. Email masking allows you to give out an email address that forwards to your "real" address, while still keeping your real address private. This has several benefits. First, it stops spammers, data miners and hackers from knowing your real email address and lets you use unique usernames on all your online accounts.

There are several services out there that provide email masking. Over the next few issues of the Update we are going to look at the three biggest: 33Mail, Blur, and NotSharingMy.Info. In this Update we are going to dig into **33mail.com.**

This service allows you to create a custom domain. Our example is "@touchpoint.33mail.com". Now when we want to give out an email address, we make something up, like this: **newsletter@touchpoint.33mail.com**

Pros: The obvious benefit to 33mail is you can make addresses up on the fly. You don't have to log in and create them.

Anything you put in front of your custom domain will forward mail to you. Another benefit is that you can make them descriptive, and you can have as many as you want. This allows you to easily keep track of what each address was used for. If you start getting spammed from an address, 33mail let's you turn forwarding off.

Cons: Because all of your 33mail addresses use your custom domain, they can all easily be linked. This takes away a lot of the privacy afforded by these accounts. Also, because any email address to your custom domain will forward to you, you can be spammed pretty easily. All it requires is that someone find your domain. They can then make up an unlimited number of custom domains to send mail to.

33Mail.com isn't our favorite option, but it is nice to have something that you can make up on the fly and give out without a second thought.

Upcoming Events:

Ft. Gordon Cyber Security & Tech Day

19 October 2016, Augusta, GA

Law Enforcement Intelligence Units

1-5 May 2017, Bloomington, MN

For more information go to www.tpidg.us

The easy button >>>

SCILock

The SCILock (pronounced "Sky-Lock") is a hard drive with a frozen operating system. It only allows changes in RAM but not the operating system. When you reboot your computer, the OS resets back to the original image it had on it before you booted into it in the first place. The only way to save files to the drive is to have the encrypted "admin key" plugged into the drive when you boot it up. Every time an update comes up or you need to install an application, you need to boot with this admin key. Otherwise, any files you need to save can be saved on the unfrozen data drive that is paired with the frozen drive. This means everything you did including create files, logs, browsing history is purged on shutdown and doesn't exist when you reboot.

It's almost as if you never did anything to the image and when you reboot you have this new and pristine OS image. This can be very useful and here is how it can be accomplished: Set up a good image of Windows, browse the internet normally, shut down when you click on a bad link and get your computer infected. This is much better than cleaning a dirty OS image because the files were never actually written to the drive, so you can be sure all the files are completely gone from the drive.

This can be good for operational uses as well. Instead of using a live Linux distro to leave no trace (like TAILS, which we teach in our Non-Standard Communications class), you could install Windows to the drive and it would act like a live image. One issue we see is with the data drive, which would be vulnerable to exploitation. FDE (Full Disk Encryption) would be a good idea to protect the information on that drive. Unfortunately, it seems the drive is all

Continued on next page.

SCILock

Continued From Previous Page...

or nothing when it comes to the OS drive and the data drive, so you can't just have an OS drive. It would be nice to have the capability to take the data drive out because that seems to be one of the only weak points. It would be nice to have an external or even a flash drive form factor with just the OS drive to carry around and be able to boot into your own custom, unchangeable Operating System when necessary. In its current form factor, we see non-tech savvy users and even some savvy users not wanting or not being able to use it, specifically the laptop version, because they would need to replace their current hard drives with the SCILock. Every time an update comes along, the user would need to open up their laptop, plug in the admin key and leave their laptop open while the updates are installed (the 3.5" desktop version has a solution for this). Because of this inconvenience, users are likely to probably ignore the update warnings every time they boot up to avoid going through all of the trouble of updating. A way around this would be to allow the updates to go through, keep the computer on for weeks at a time and pray that the power doesn't go out and your battery doesn't die. But as soon as it reboots, you're back to square one.

The technology behind the SCILock could be revolutionary, but in its current form factor, we find it to be impractical for the end user. The only way you would get an average user to use this would be if you installed it and maintained it for them. Even then, we think it would frustrate them to have to save their personal files to a separate drive. In a corporate or government environment, we can see this being worth installing in employee workstations as a hardware alternative to something like Deep Freeze. This is a far more robust solution than using virtualization software. Though virtual machines offer a very strong level of security, malicious files can escape and infect the host operating system by very sophisticated malware. There is absolutely no such concern with the SCILock drive.

All in all, SCILock is definitely worth using if you have time to maintain it, or if you are operating under exceptionally high risk. We would definitely like to see an expansion on the technology behind the device. For more information on the SCILock, contact us at admin@tpidg.us

coming soon >>>

In Future Issues...

Synology NAS

Special Windows 10 Edition

- Encryption

- OS Hardening

iTunes Backups

Brute Forcing Concerns Underscore Need for FDE

Earlier this week a vulnerability was discovered in iTunes backups. If you backup your iPhone, iPad, or iPod Touch to iTunes, you have the option to encrypt it. The vulnerability allows an attacker to brute-force the encryption password at up to 40 times greater speeds than what was previously believed. There are two big takeaways from this.

1. Password length and strength matters! We preach this in our Digital Protection and Non-Standard Communications courses, and this is a good example of why. Use good passwords on everything. If you're using a password manager, it's easier.
2. Full-disk encryption matters! Do we hope this vulnerability is fixed soon? Of course. Are we terribly worried about it in the meantime? Nope. The iTunes backup is still on a full-disk encrypted computer and only stored locally.

Even if a program is "secure" now there will probably come a time when it isn't. Using best practices and defense-in-depth is important even if it doesn't seem like it now.