in this issue >>> V.1.4

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- WhatsApp Encrypting Messages End-to-End with Signal Protocol
  - WhatsApp Blog
- Use an Ad-Blocker! Ads on Big-Name Sites Used as Malware Vectors
  - Ars Technica
- Update Your iOS Devices to 9.3.1; Exploit Can Kill Apple Devices Running Older Versions
  - Krebs on Security
- "BadLock" Bug Probably Not as Bad as we Thought
  - Naked Security
- Checksums Updated 15 April 2016
  - Your Ultimate Security Guide

The BRCK:

Austere Environment Wi-Fi Hotspot

- Jacob Alexander

Touchpoint has been teaching various tactical uses of the BRCK for just over 18 months. The BRCK is an "austere environment" Wi-Fi router that has the ability to use existing network infrastructure, whether it's Wi-Fi, Ethernet, or 3G GSM connections, and gives you the capability to access the internet. The BRCK was originally designed in Kenya and operates as a router/power supply, but has many more capabilities than that.

What's great about this device is it creates its own LAN (Local Access Network), which allows you to file share, easily connect to your other devices. For added security the BRCK also segregates your traffic the network that you will be using to access the internet. The BRCK (which we obviously call "the brick") also features an very capable 8000 mAh lithium-polymer battery. Not only is the device self-powered, its USB port can also be used to charge other devices if needed. This is a huge value added in remote areas.

The device itself is rugged and dust-proof, which allows you to take it anywhere without fear of damaging the device. The management of the device is done so through a cloud based interface, which while not ideal from a security standpoint, works very well and is very user-friendly.

Overall, the BRCK is a neat, rugged, little device that is portable and can be used anywhere. Some improvements could be made, such as an upgraded cellular modem and an offline management mode, but we hope to see that in BRCK 2.0. If you have recently attended our NSC or COTs courses, you have used this device as a hotspot for digital tradecraft, or to push live video through COTS devices. For information about non-standard uses for BRCK contact admin@tpidg.us.

www.brck.com

set the stage >>>

ID Management 101 (Part 4 of 5)

In the first part of this series we discussed conducting a self– assessment. In part two we discussed the importance of NOT giving information out, and last week we talked about removing data.

Disinformation

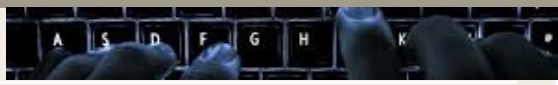
This week we will talk about elevating your ID management game by creating disinformation. When someone searches for you online, he or she expects to find something. If you have removed your personal data from the internet totally you will be more interesting for being a "black hole". Rather than let the data brokers and advertisers decide what information is available you can choose to without compromising yourself.

Disinformation is false information **that does not endanger anyone else**. If someone with bad intent searches for your home address online they will find a lot of false leads. We realize this technique may seem a little sketchy, but trust us, it works.

Creating Disinformation

You create disinformation by using data marketers tactics against them. When you get a retail loyalty card or subscribe to a magazine, they get your name, home address, and the products you buy. When you sign up for your next discount card, use a non-existent address (we reiterate—NOT someone else's address). When you sign up for your next magazine subscription, use your real home address with a false name. These results will soon start populating in online search results for your name and protecting your true home address.

The easy button >>>



Wickr: Encrypted Text and IM

If you are a graduate of our NSC or Data Protection courses then you understand the importance of protecting the content of your text and instant messages. When discussing important plans or details it is important to protect the content of those communications. Wickr allows an easy way to do it.

We have used and recommended Wickr for a long time in our Non-Standard Communications, Data Protection, and Identity Managment courses. Wickr is an ephemeral messaging system that automatically encrypts your conversations with very strong AES-256 encryption. Your messages are also automatically deleted at an interval of your choosing; 24 hours is the default but this may be increased to 6 days or lowered to 5 seconds.

We mentioned Wickr a couple issues ago in a segment on mobile apps, but there has been a major change to this product that you should be aware of. Wickr Me was recently rebranded. Along with the rebranding Wickr also introduced paid enterprise solutions (Wickr Professional) which gives Wickr a clear revenue stream. Wickr also introduced a new logo. If you've had the app for a while and suddenly see a new logo (shown at right) on your device, don't worry.

Despite the change Wickr Messenger is still our go-to encrypted messaging app for Android, iOS, Windows, Linux, and OS X. It's secure, it's user-friendly, it's growing in popularity, and it's free. For more information visit https://wickr.com.

Upcoming Events:

-SOFIC 23-26 May 16
Tampa, Florida
-Blackhat 30 July-04 Aug 16
Las Vegas, Nevada
-NATIA 09-15 July 16
Seattle, Washington

For more information go to www.tpidg.us

Threat Modeling: An Intro

If you have attended our Non-Standard Communications course you know that every mitigation we teach is guided by systematic threat modeling.

Choosing effective digital mitigations is important, and ensuring they are effective is a function of knowing who and what they are designed to defeat. It is also knowing how they make you "look" to an adversary. If you look too defensive you may inadvertently target yourself for more aggressive monitoring and exploitation—something you don't want no matter how good your interventions are. Understanding your threat is a function of threat modeling. Threat modeling means knowing several things:

1. Who are the threat actors?
2. How do I look to them?

Who are the threat actors? Understanding who the threat is can give you insight into the motivation behind the threat. Are you trying to hide from a jealous ex-spouse? Are you trying to operate under the nose of a foreign government? The motivations these two actors display may be very different, and their capabilities certainly are. Estimating capabilities ity is important; underestimate and you get compromised, overestimate and you stifle

your own ability to operate. Choose your mitigations based on the answer to this, and the next, question.

How do I look to them? This must be answered honestly, and you must view yourself through *their* lens. Do you look suspicious? Would you keep an eye on yourself if the shoe was on the other foot? Have you been compromised in the physical world, causing them to be more interested?

If the answer to any of those "sub-"questions is "yes", the cycle starts again. Re-evaluation should be an ongoing, unceasing process throughout your operational cycle.

Remote Access Tools

Remote Access Tools (RATs) are a particularly insidious form of malware. RATs are incredibly powerful and can remain unnoticed on your system for months or years.

RATs & RAT Traps

Remote Access Tools are aptly named. They are implants that give an attacker persistent (ongoing) access to your computer. They also give the attacker the ability to control certain aspects of your computer's behavior. This includes turning on your webcam or microphone, capture your key strokes, and more. RATs are typically spread through pirated software, music, and movies, and malicious email attachments.

The best way to prevent infection with RATS is by modifying your behavior. Don't download pirated stuff—not only is it illegal, it's also asking for an infection. Don't open email attachments from people you don't know, and if you get one you weren't expecting contact them and ask them if it's legit before you do open it. It's also not a bad idea to run an antivirus application like Avast or Avira, and scan your computer periodically with something like Malwarebytes Anti-Malware or Spybot Search and Destroy.

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

Course Spotlight: Family Digital Safety Seminar

In today's digital world, service members are trained to reduce risk of digital compromise to ensure both unit and mission safety. The digital world is unique because it crosses boundaries into the home and into the work environment. Not only can mission compromise start at the home but issues caused in the digital environment, such as Identity Theft can affect the service members performance in the work place. TouchPoint offers a Family Digital Safety Seminar for military and Police/Fire/EMS personnel that gives family members the tools to communicate securely with their loved one, protect themselves against threats like identity theft, and understand the risk of social media. A two-hour awareness class is included with our Non-Standard Communications courses and 1– and 2-day full seminars are available. For more information contact us at admin@tpidg.us.

coming soon >>>

In The Next Issue

The TOR Network
COMSEC: Silent Circle
Hardware Two-Factor Tokens
SSL and Why it Matters