in this issue >>> V.1 /I .2

Offensive Tools Review

Raspberry Pi 3 First Look

ID Management 101, Part 2

Mobile Security App's

Passwords/Password Management

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

Threat Alert: Cryptoware>>>

If you didn't need a good reason to already, you should be running a capable anti-virus application. One type of malicious software (malware) that such an application could defend you against is called "cryptoware." Cryptoware installs itself on your computer through malicious downloads or internet links, then begins encrypting your files. If it is your personal computer these are likely precious family photos, medical and financial information, and other personal files. If it is your work computer these could include crime scene photos, reports, and other critical information.

Once the files have been encrypted you must pay a ransom (currently around 1 BitCoin, or the equivalent of $400) to receive the key to decrypt your files. If you don't pay the ransom, your files will be permanently deleted with no hope of recovery. Several law enforcement agencies have fallen prey to such malware.

If you do not have an anti-virus application we recommend using Avast. It is free and performs exceptionally well in independent tests.

Mobile Security App's

Best Practice for Mobile Devices

Smartphones make us incredibly vulnerable. They allow us to be tracked, their cameras and microphones can be hijacked, our browsing and message traffic can be intercepted. We can help stop some of this through the use of apps.

Before I go on I should point out that many apps introduce more vulnerabilities than they fix. Apps spew unencrypted data back to their authors. Apps frequently have permissions to access your camera, microphone, contacts, Wi-Fi networks and location data. Generally speaking you should strive for less, not more, apps, but there are some that can help.

-***Wickr Me***: Wickr Me is a very secure ephemeral messaging system. Wickr Me protects your messages through "their entire life cycle", device to device. Your messages also expire and are securely deleted at a user-defined period of time from 3 seconds to 6 days. This means that you and the people that you are messaging aren't carrying around months worth of sensitive communications. Wickr is free and is also available for desktop Windows, Mac and Linux. For more information visit Wickr.

Wickr
ESCAPE THE INTERNET®

https://www.privateinternetaccess.com/sguide.

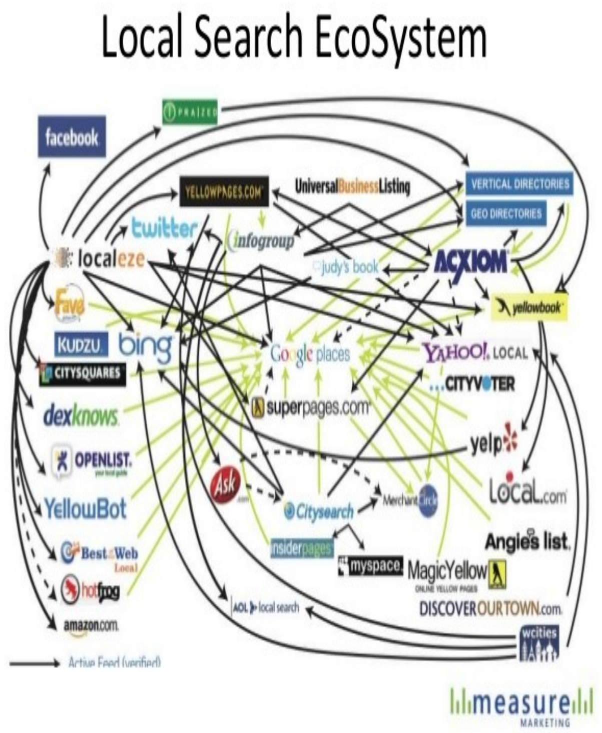
-Google Authenticator: If you use two-factor authentication you probably already know about this one, if you don't we'll talk about two-factor in the next issue. This app allows you to carry your second-factor codes on your device rather than waiting for a text message. This is especially helpful in areas where you may not have phone coverage. This app is free and available in on Google Play.

- Private Internet Access: Private Internet Access is a virtual private network app that encrypts all your device's data traffic. This offers an excellent layer of privacy and security and this is the most user-friendly one we've tried. PIA costs as little as $3.33/mo and is available at https://www.privateinternetaccess.com/sguide.

set the stage >>>

ID Management 101 (Part 2 of 5)

In last issue we talked about stopping the bleeding and conducting a self-assessment. Even if you are only a “light” Facebook user, or even if you don’t use it at all, there is a very good chance you found a great deal of your personal information publicly available on the internet. Still not convinced? Go to https://thatsthem.com/ and search your name and state of residence. The next step is critical and perhaps most effective step in the Identity Management process. The next step is to assess your level of exposure. If you have attended one of our courses you know the mantra: STOP GIVING OUT YOUR INFORMATION! Rather than give out your home address, get a Post Office Box. Get a Google Voice number that will forward calls to your phone and give that out instead of your mobile number. Use www.33mail.com to create instant, disposable email addresses that forward to your “real” account. Taking these simple steps may not seem like much, but the longer you continue to give your information out, the harder it will be to clean up.



The easy button >>>

Passwords and Managers

While passwords are a vital component of system security, they can be cracked or broken relatively easily. Password cracking is the process of figuring out or breaking passwords in order to gain unauthorized entrance to a system or account. It is much easier than most users would think. (The difference between cracking and hacking is that codes are cracked, machines are hacked.) Passwords can be cracked in a variety of different ways. The most simple is the use of a word list or dictionary program to break the password by brute force. These programs compare lists of words or character combination against passwords until they find a match.

Most of us in the security community assume that password managers are like seatbelts: everyone uses them. Unfortunately, this is not the case, but it should be. Here’s why: To be effective, passwords have to be both long and complex. What is long? Twenty characters would be a good minimum. What is complex? Put simply, if you can remember it probably isn’t complex enough. This would be hard enough if this was the end of the story but it’s not: all of your passwords should also be different. Yes, every account you have should be protected with a different password. If one password is broken, leaked, or socially-engineered it could lead to the downfall of many of your accounts. This happened to Mat Honan and he explains it in the article linked below. How do you manage a password that is long, complex, and different from all the others? With a password manager, a small program that encrypts your passwords safely on your computer until you need them. There are many out there but we recommend the following: if you use Windows try Password Safe (https://www.pwsafe.org/). If you’d like a cloud-based option try LastPass (https://lastpass.com/). For everything else there is a branch of KeePass that will work for you, www.keepass.info.

Mat Honan Article: http://www.wired.com/2012/11/ff-mat-honan-password-hacker/

Password MGR App:

Codebook Secure Notebook: Codebook is one of the best, most secure password managers out there and it works extremely well on Android and iOS devices, as well as Mac and Windows desktop computers. The mobile apps securely store passwords and notes and have a number of convenient features, like syncing databases with other devices locally over Wi-Fi. Codebook Password Manager and Data Vault is available through the App Store and Google Play. For more information visit https://www.zetetic.net/codebook/.

Intro to Offensive Tools

RaspberryPi

-Kali Linux

Kali is yet another distro that Linux has to offer, except this one comes with all of the tools a white hat hacker would ever need. As with all Linux Distro's, it can be run from a CD or USB drive, allowing full control over the victim machine. This operating system designed by Offensive Security has many open source tools ranging from wireless attacks (aircrack-ng suite) to stress testing (mdk3) to sniffing internet traffic (Wireshark). Kali comes in several different versions including a light version and a version that runs on ARM processors. It also now offers the ability for full customization of which tools are included in the live image allowing specific purpose images. Overall, Kali Linux is a versatile, well-rounded penetration testing operating system for the avid white hat.

-Rubber Ducky

The USB Rubber Ducky is a brilliant device created by Hak5. It appears to be just an ordinary flash drive, but the computer you plug it into recognizes it as a keyboard. For the tech geeks out there, this is accomplished by modifying the USB firmware of a storage device and changing it to that of a keyboard. The fact that it is recognized as a keyboard makes the computer trust it as such, allowing custom scripts with key combinations to ran on mount. Even the newest pen tester has the ability to use this device with the hundreds of already written scripts for the device. There are thousands of predefined scripts, some download files and some enable remote access to the victim machine. A more advanced pen tester can write their own scripts and get the computer to do basically whatever they want.

-Wi-Fi Pineapple

The Wi-Fi Pineapple is another device created by Hak5. It operates as a malicious router that can act as an evil twin or rogue access and then used to perform man in the middle attacks to gather information or to exploit the victim. The Pineapple is perhaps more suited for the advanced pen tester, but it is very user friendly and easy to figure out. Tools are added as modules in almost the same way you would add apps to your phone. There are a great many tools that can be used on the Pineapple such as: nmap (recon), ettercap (MiTM), sslstrip and deauth. There are millions of possibilities with this device and hours of enjoyment for the expert pen tester.

Raspberry Pi 3

The Raspberry Pi 3 builds on an already brilliant device that serves a lot of unique purposes. The Pi 3 is more powerful, adds built in Wi-Fi and Bluetooth, and keeps the same form factor as the previous generation, which means your Pi 2 cases will still work. The wireless card used is a Broadcom BCM43438 which supports 802.11n and Bluetooth 4.1. This chipset currently does not support monitor mode, so more advanced users will have to purchase a separate Wi-Fi dongle. Its' performance boost is achieved with upgraded RAM speed (900 MHz), a faster processor (1.2 Ghz), and 64-bit architecture (the Pi 2 had 32-bit architecture). The fact that such a small device is so powerful, gives it infinite uses. Touchpoint is currently teaching the Raspberry Pi as a COTS solution for the following: surveillance video capture, Virtual Private Network, vehicle tag, and as a MAC address sniffer.

-SOFIC 23-26 May 16
Tampa, Florida

-Blackhat 30 July-04 Aug 16
Las Vegas, Nevada

-NATIA 09-15 July 16
Seattle, Washington

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

coming soon >>>

In The Next Issue

ID Management 101 Part 3

Thirty-Day Digital Security

Virtual Private Networks

Two-Factor Authentication

Threat Alert: RATs

The information in this issue was contributed by the following members of the TPIDG team:

Justin Carroll
Special Activities Program Manager
J.carroll@tpidg.us

Jacob Alexander
InfoSec Instructor/IT Manager
J.alexander@tpidg.us