in this issue >>> V. 2.06

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- If Your iPhone is Stolen, Beware of iPhishing Attempts
  - Krebs On Security
- Print Out the EFF's Border Search Pocket Guide Before You Travel
  - Lifehacker
- Supply Chain Attack: Malware Found Pre-Installed on Some Android Phones
  - Ars Technica
- Yahoo! Cookie Hack Effects 32 Million Accounts
  - Ars Technica
- Apple Aggressivley Pushing Two-Factor for iOS 10.3 Users
  - Naked Security

The CIA "Vault 7" Leaks

What You Need to Know

Major news broke last week with the release of thousands of documents from the Central Intelligence Agency. These documents were released by Wikileaks and referred to as the "Vault 7" collection. Of the almost 8,700 documents that were leaked, many were unclassified but For Official Use Only (FOUO). Some of the information was classified at the Secret level, and a very small percentage was protected with higher classifications. Many major news outlets, unsure of how to analyze the information they now have access to, are making inaccurate reports. Some headlines claim that the CIA has hacked everything from smart TVs to the encryption in Signal Private Messenger.

- **Breaking Encryption**: Some articles have indicated that the CIA is capable of breaking the encryption on popular messaging apps like Signal and Wickr. This is false; what the report actually says is that the agency can bypass such encryption by infecting the phone with malware and intercepting the message as it is being created. The encryption has not been compromised and can still be trusted.
- **Interfering with antivirus applications**. One of the more alarming items in the Vault 7 archive is the ability of attackers to interfere with antivirus programs or "Personal Security Programs" (PSPs). These types of attacks prevent PSPs from alerting the user to suspicious behavior or blacklisted applications. This does not mean that you should not use a PSP. They still provide a lot of protection from other forms of attack but they should not be relied upon totally.
- **Smart TV Hacking**: One of the more sensationalized and widely-reported items from the Vault 7 leaks said that smart TVs could be hacked. Hacking the TVs, turned them into listening devices by using their embedded microphones, and the information captured was transmitted via the TV's internet connection. This one is credible and has been well-known in the hacking community for several years.

Continued on next page >>>

set the stage >>>

The CIA Vault 7 Leaks

<<<Continued From Previous Page

- **Hacking Windows, Mac, and Linux computers, Android and iOS Mobile Devices**: It was also widely reported that the CIA possessed the capabilities to hack computers and mobile devices across a wide range of operating systems. We view this as fairly accurate, but many of the exploits rely on outdated versions of software. Some zero-day exploits were discovered in Vault 7, but Wikileaks has not made them fully public yet on the grounds that they are releasing to manufacturers and giving them an opportunity to patch first.

What does this mean for you? It is unlikely that any reader of the Digital Update is being targeted by the CIA. However, there is some actionable information here. Knowledge of the vulnerabilities out there can be used to threat model other adversaries because similarly well-funded intelligence organizations likely have similar capabilities. If you are in the military, intelligence community, or law enforcement, this gives you an idea of what you may be working against—and how to defend against it. See the final page of the Update for some information on how to protect yourself from similar attacks.

The Vault 7 leak is one of the biggest dumps of intelligence data we have ever seen. However, much of what has been reported is sensationalized by the media to drive web traffic, and some of the headlines we have seen are totally inaccurate. To view Wikileaks' summary of the Vault 7 documents or to view the full archive, visit **https://wikileaks.org/ciav7p1/**

Upcoming Events:

Law Enforcement Intelligence Units

May 1-5 2017, Bloomington, MN

Associated Locksmiths of America Expo

June 16-22 2017, Rosemont, IL

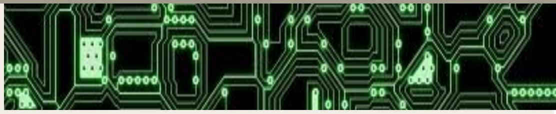
National Technical Investigators' Association (NATIA) Annual Conference

July 12-23 2017, Tampa, FL

BlackHat USA

July 22-27 2017, Las Vegas, NV

The easy button >>>



Encrypted Messaging Protocols

Our Recommendations

We review a lot of apps and services in the Digital Update, and we have covered a number of encrypted messengers in the past. With the recent CIA/Wikileaks news, we thought it would be a good time to go over the encrypted communication apps that we teach in class and use in our personal lives.

RECOMMENDED

Signal Private Messenger. Signal is free and offers some of the strongest encryption available with its unique "Signal Protocol". The features we mentioned in the last update (video calling and iOS CallKit support) have now been implemented in a full release. Our only complaint: the desktop version is a Chrome add-on that only supports messaging.

Wire Private Messenger: Wire is quickly becoming a favorite because it supports text, voice, and video and is available as a standalone app for Windows, Mac, Linux, Android, and iOS. If you can't (or don't want to) install the app you can also use Wire from a web login.

ProtonMail: ProtonMail is our mail provider of choice. ProtonMail offers end-to-end encryption as a baseline feature. Premium accounts have access to a number of other features including alias email addresses and custom domains.

NOT RECOMMENDED

Wickr: We have taught Wickr in the past but are slowly backing away from it. We don't believe there is anything wrong with it, but there are too many other options out there that offer expanded features for us to recommend a single-use item.

Surveillance Defense

Protecting Yourself from Vault 7-Style Attacks

The CIA Vault 7 leaks are alarming, but there are ways to defend yourself against attacks like these. Since TouchPoint works for the US Government, we aren't worried about the CIA, but attacks similar to these are available to many well-funded actors. The exploits may not be exactly the same, but the capabilities are probably very similar. The following are ways you can protect yourself:

1. **Keep your OS and applications up-to-date**. This isn't anything new. We've said it here in the update before, but outdated software is a major attack vector. Running out-of-date software means that an attacker doesn't have to use a zero-day attack to exploit your device and makes you a soft target.
2. **Audit the applications on your machine**. Go through your programs and get rid of any anything you haven't used in the last month. If you really need these programs later, you can install them again, but keeping your programs to a minimum reduces your attack surface significantly.
3. **Run a Standard User account**. Using an administrator account for day-to-day use is bad because any malicious code that makes it to your computer (from a website, an infected USB drive, a malicious attachment on an email, etc.) will find itself in an environment with administrator privileges where it can execute. Using a Standard user account will give you an excellent layer of protection.
4. **Use antivirus software**. Many of the Vault 7 documents discuss the CIA's ability to manipulate antivirus software so that an intrusion will not raise an alarm. This is true—antivirus won't catch everything, but you should still use it. You will make an attacker's job much harder, and you will greatly reduce the risk of lower-level malware on your computer. We recommend Avast Antivirus in our Non-Standard Communications and Digital Protection Courses.
5. **Use encryption**. The Vault 7 leaks demonstrate that encryption works. It forces hostile actors to exploit your device which is much more targeted, intrusive, and risky. Use full disk encryption and encrypt your communications.

These steps will not make your computer 100 percent secure. You still have to use some basic best practices: be cautious of links contained in emails, text messages, or sketchy websites, don't download and open attachments from people you don't know, and don't "plug and play" with USB devices. These steps will still make you a much harder target for malicious actors.

The Complete Privacy & Security Podcast

TouchPoint's Justin Carroll and Michael Bazzell, the authors of the *Complete Privacy & Security Desk Reference*, have recently started a podcast. The show, called The Complete Privacy & Security Podcast, covers a range of topics that would be of interest to readers of the Digital Update.

Justin is TouchPoint's primary instructor for Non-Standard Communications, Digital Protection, and Active Identity Management courses.

If you have attended any of these courses you know how rapidly technology changes. This podcast is a great way to stay current on the latest tools and tactics to keep your data safe.

The Complete Privacy & Security Podcast is released weekly. The show notes for each episode are available on **Justin's blog**. Subscribe today on **iTunes**, **Google Play**, **Stitcher**, or in your favorite podcast app.

coming soon >>>

In Future Issues...

Internet Browser Comparison

- ⇒ ***Chrome, Firefox, Opera***
- ⇒ ***Mobile Browsers***

Firefox Setup Review

Browser Extensions

If you would like to see a specific a product or service reviewed in the Digital Update, please don't hesitate to get in touch. We are always looking to make content as relevant as possible to our readers. You can reach out to us through the TPIDG.us or email directly to admin@tpidg.us .