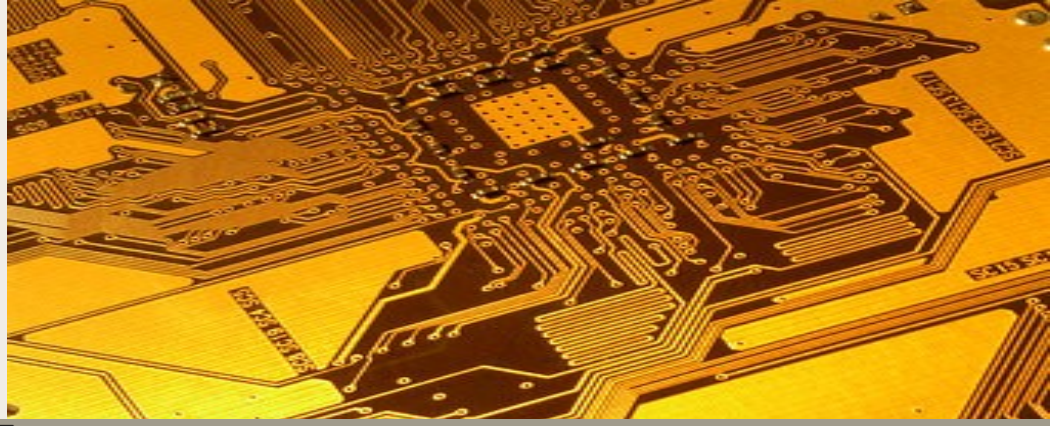
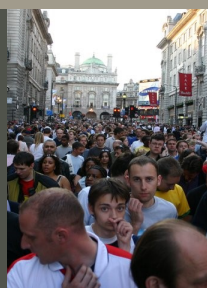
in this issue >>> *V.1 /I .1*



TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update



current topics >>>

In the News:

-Judge confirms CMU scientists were paid by the FBI to hack TOR.

-ASUS facing audits for poor Wi-Fi router security.

-Apple hires developer from the secure messaging application Signal.

-German police given go-ahead to use home-brewed spying Trojan

Verifying File Integrity

Checksum Calculator

Welcome to the first edition of the Touchpoint Digital Update. Our newsletter will be your source for digital security and identity management news. All newsletters can be downloaded from our Website and new updates will be sent out twice per month, on the 1st and 15th.

File verification is the process of using an algorithm for verifying the integrity or authenticity of a computer file. Our Non-Standard Communications and Digital Security courses teach the verification of executable files before running them. We do this using a checksum calculator, a simple tool that verifies the file has not been tampered with. (An article detailing how to do this is available here.) For a link to the checksum repository click here.

By themselves ,checksums are used to verify data integrity, but they should not be relied upon to verify data authenticity.

Checksums are used to verify data integrity, but should not be relied upon to verify data authenticity.

This week we saw an excellent example of why this is important. The website of a popular operating system, Linux Mint, was hacked. The attacker replaced the download link and anyone who downloaded this OS on February 20th inadvertently downloaded a faulty version with a security hole that gave the attacker total access to the device running it. A simple checksum verification would have revealed the download as fraudulent.

This underscores the need to validate files before trusting them. The official press release on this attack is available here.

https://yourultimatesecurity.guide/checksums.html

set the stage >>>

ID Management 101 (Part 1 of 5)

While America was fully engrossed in the Super Bowl, hackers were hard at work Doxing 20,000 FBI agents and 9,000 Homeland Security employees.

Stop the Bleeding

If you haven't started cleaning up your online presence or are still using the default settings on your phone and laptop, then you are hemorrhaging personal data. This data includes your address, your relatives names and their addresses, your children's Facebook profiles, the routers that your phone has connected to that show your pattern of life. All of this information makes you targetable, for some the threat may be reporters after an officer involved shooting and for others it may be by ISIS publishing your data on Jihadi forums. The methodology for protecting and eventually manipulating your digital footprint is the same for both of the situations mentioned above but it needs to start today. The first step in Active Identity Management is the Self Assessment.

The Self Assessment

Before you can begin removing your information, you must know what information is out there about you. Conducting a self-assessment is the first step in the process. Begin by searching for yourself on common search engines. Use quotations around the information you are searching for more accurate results. Search your name, home address, phone number, and email address(es) and usernames and document everything you find. Be warned - you will probably be uncomfortable with how much information you find.

Malware >>>

Emerging Threats

If you are a graduate of our NSC or Data Protection courses then you understand the importance of Threat Modeling. The list of threats outlined below will help you more effectively conduct threat analysis and protect yourself from both state and non-state actors who are actively targeting data.

-Nominal ISIS supporters continue their practice of hitting small targets of opportunity, this time a small manufacturer of solar panels in England. The "Caliphate Cyber Army" defaced the website of Solar UK at the end of January.

-The Internal Revenue Service announces an increase (of 390,000) to the number of taxpayers whose information was stolen from poorly secured IRS sites.

-In Q4/15 there was a noted surge in polymorphic malware, with 97% of malware morphing to become unique to a specific endpoint device. By changing attributes to evade detection, polymorphic threats pose a major problem for traditional, signature-based security approaches, which often fail to discover singular variants.

-A report released on February 26 concludes that an attack on the Ukrainian power grid was coordinated and highly sophisticated. The attack caused a black-out for over 225,000 Ukrainians by hitting three separate regional power distribution companies within 30 minutes of each other. A team of US cyber officials said that the hackers conducted "extensive network reconnaissance" and delivered malware via phishing attacks months before delivering the "BlackEnergy" virus which caused the black-out.

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

Essential Software for Data Encryption

Encryption is an inestimably important part of a good digital security posture. Encryption protects your data by making it inaccessible to anyone without the correct password. Using encryption can be daunting, but there are some user-friendly products that we recommend.

Data-at-Rest: Data-at-rest is the information on your computer, hard drives, or smartphone. The program we recommend is VeraCrypt. VeraCrypt is a versatile, full-featured encryption software. VeraCrypt works on Windows, Mac, and Linux operating systems. It is also free and open-source and available here.

You should also encrypt the data-at-rest on your smartphone. If you have an iPhone this is as simple as requiring a passcode on the device, which can be as long as 30 digits (the longer the better). If you have an Android phone ensure you have a passcode enabled. Next, open your settings, and tap Security". Scroll down until you see Encrypt". Plug your device in and allow up to an hour for the encryption process to occur.

Data-in-Motion: Data-in-Motion is your information that is sent via voice, text, and email. There are applications and programs that can protect all of these forms of data-in-motion. For encrypted voice conversations and text messaging we recommend Signal. You can find more information here. For encrypted email we recommend switching your email provider to Protonmail or Tutanota. Both of these options are free and encrypt your messages end-to-end.

Intro to Linux Distro's

In each issue of Digital Update, Touchpoint will introduce a series of hardware and software solutions that will assist the readers in securing themselves or conduct ng offensive security applications. Today we will be discussing one defensive and one offensive Linux Distro.

Privacy…..

JONDO Linux- JonDo offers a secure, preconfigured environment for anonymous surfing and more. It is based on Debian GNU/Linux. The live system contains proxy clients for JonDonym, Tor Onion Router and Mixmaster remailer. JonDoFox is a preconfigured browser for anonymous web surfing and TorBrowser is installed too. Thunderbird for e-mails, Pidgin for anonymous instant messaging and chats, TorChat, LibreOffice , GIMP and Calibre for eBooks.

Pen Testing….

KALI Linux- Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools aimed at various information security tasks, such as Penetration Testing, Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

In addition to our non-technical training deliveries, Touchpoint also delivers the following training programs that focus on subject matter within the Computer Network Operations (CNO) training spectrum:

- Raspberry Pi Basic Course (1 week)
- Raspberry Pi Advanced Course (1 week)
- CNO Course (6 weeks)
- Wi-Fi Attack Course (2 weeks)
- Basic Identity Management (3 days)
- Advanced Identity Management (5 days)
- Social Media Exploitation (1 week)
- Basic Non-Standard Comm's (1 week)
- Adv. Non-Standard Comm's (1 week)
- Data Protection Course (1 week)

Contact Touchpoint at info@tpidg.us or call 910-322-8805 for more information.

coming soon >>>

In The Next Issue

Offensive Tools Review
Raspberry Pi for Data Protection
ID Management 101, Part 2
Mobile Security App's
Passwords/Password Management