MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THE DARK WEB: WHAT, WHERE AND HOW?

Connie G. Mastovich -- Senior Security Compliance Analyst, Reclamere, Inc.

Rachael Lucas -- Project Manager, Reclamere, Inc.

Connie Mastovich, CISSP
Senior Security Compliance Analyst

- ✓ **CISSP**: Certified Information Systems Security Practitioner by $(ISC)^2$
- ✓ 24 years in the I.T. department of Lee Hospital (currently Duke Life Point / Conemaugh Health System
- ✓ 8 years working for Northrop Grumman, supporting a classified Air Force contract in a Security role
- ✓ Security and Privacy Analyst at Philips Healthcare

THE DARK WEB
VS.
THE DEEP WEB

THE LAYERS

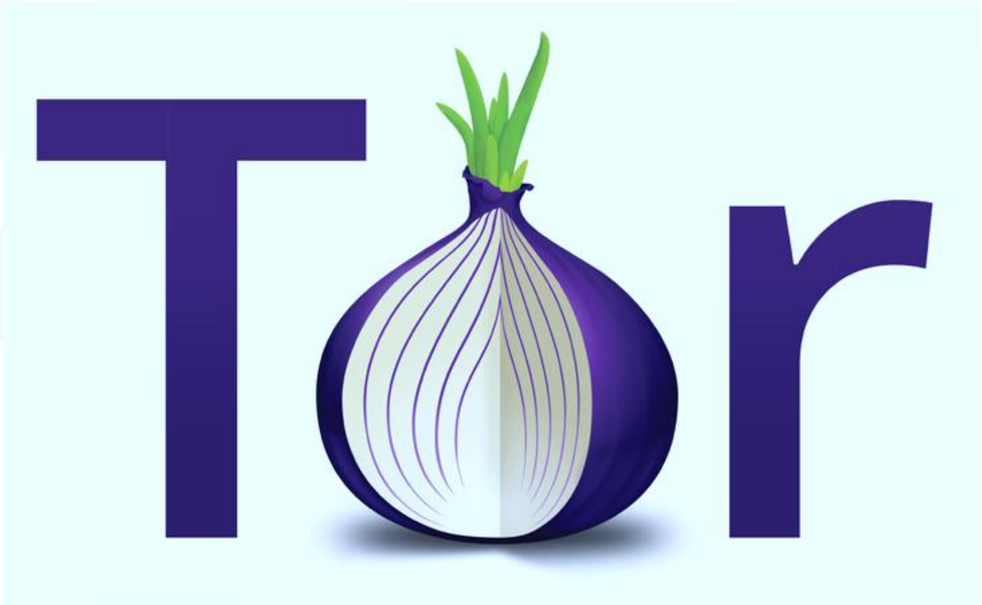
- Surface Web
  - Google and other search engines can locate
- Deep Web
  - Can not be found by any search engines, but can be found by searching a website (search boxes)
- Dark Web
  - A small portion of the Deep Web that has been intentionally hidden and is inaccessible through standard web browsers

https://brightplanet.com

HOW CAN YOU GET THERE?

- Tor: **T**he **O**nion **R**outer
  - Anonymous communication and privacy
  - Masks IP address
    - Onion Routing

- How do you get Tor?
  - Download it
  - Email them
  - Get the installation from a friend



Tor and the Dark Art of Anonymity by Lance Henderson

WHAT TOR CAN NOT DO

- Protect you from attachments
  - Includes executables, flash videos, etc.
- Cloak your identity when using real email
- P2P
  - Bandwidth intensive

ANONYMITY …… GUARANTEED?

There are no guarantees…….
But there are ways to make increase the odds of anonymity:

- Tails live OS
  - Anonymous internet usage, all connections to the Internet are forced to go through the Tor network
  - Leave no trace on the computer you are using unless you ask it explicitly, uses state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging

https://tails.boum.org/

- Spider Oak for cloud storage
  - Safer alternative to Dropbox
  - Encryption keys created client-side

ANONYMITY …… GUARANTEED? {CONTINUED}

- Whonix
  - Based on Debian/Linux
  - Also routes through Tor
  - Alternative to Tails
- Macchanger
  - Spoofs MAC address for every session
- Those layers again…….
  - Whonix or Tails, a trusted VPN, and spoofed MAC address

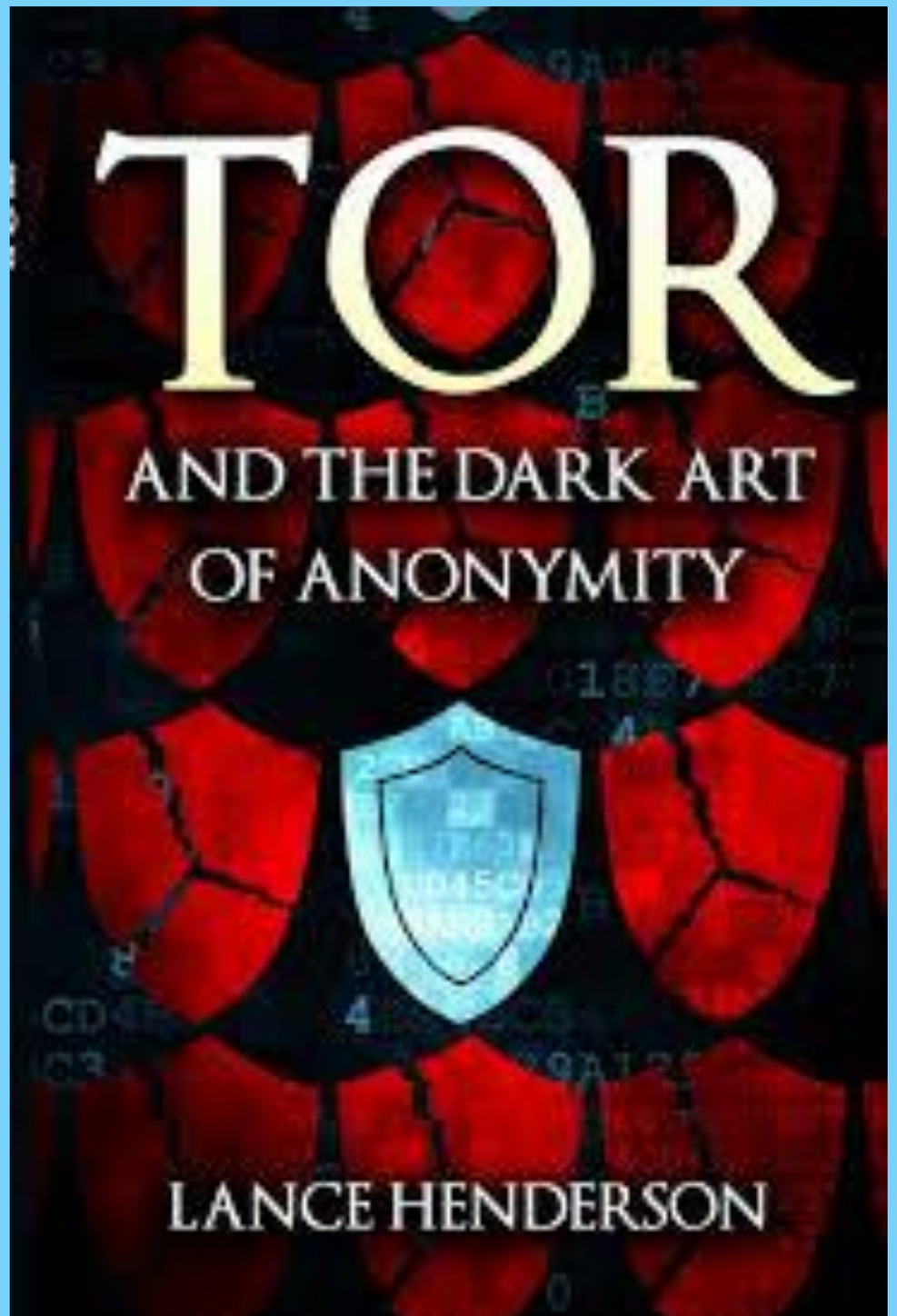
MORE TOOLS, MORE ADVICE

- Disposable MAC address
  - Can be bought
  - Included with Tails OS
- Secure VPN
  - Privacy vs. Anonymity
- Bitcoin for payments
  - Bitcoin wallets and bitcoin mixers
- Keep separate identities separate at ALL TIMES!!

WHAT IS THE ROLE OF LAW ENFORCEMENT?

- Find, identify, shut down
  - Repeat
- The Joint Criminal Opioid Darknet Enforcement (J-CODE) team
- Privacy Concerns

https://fivethirtyeight.com


TOR
AND THE DARK ART
OF ANONYMITY
LANCE HENDERSON

RACHAEL LUCAS, PROJECT MANAGER

- ✓B.A. in Advertising and Public Relations with a Minor in Marketing from Penn State University.
- ✓Compliance experience: VPP STAR OSHA Application and approval process as a Service Manager for Cintas, and R2 and NAID AAA Certifications held by Reclamere.
- ✓As General Manager, Rachael oversees the operation of the IT Asset Management division as well as the Finance and Human Resource departments. She also assists Reclamere’s Security team with project management and organization as well as policy review.

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Connie G. Mastovich -- Sr. Security Compliance Analyst, Reclamere, Inc.

Rachael Lucas -- Project Manager, Reclamere, Inc.