
worldpay
Shining a Light on the Dark Web
Matthew Heath – Sr. Threat Intelligence Analyst

The Structure of the Internet

The Internet
Made up of the indexed, searchable web

The Deep Web
Content behind some form of barrier (permissions, paywall, etc.)

The Dark Web
Hidden content visible only with specialized tools

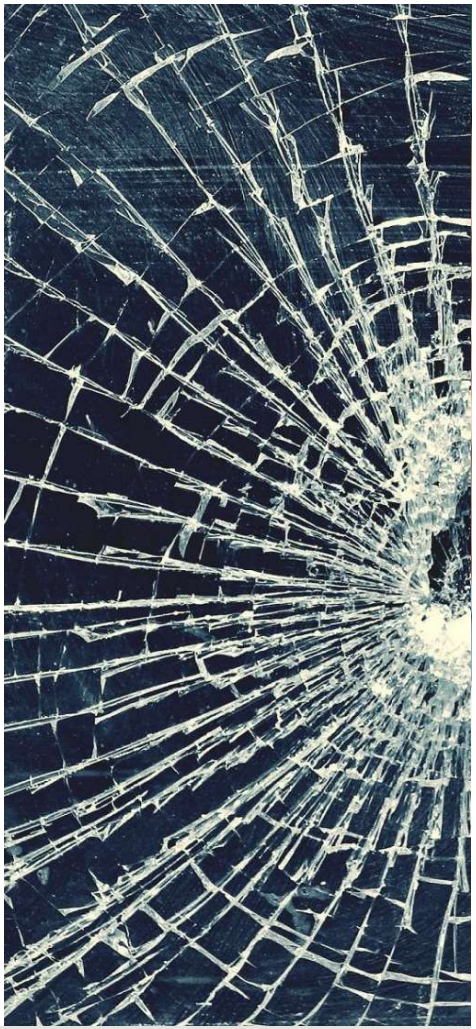
The Dark Web

Accessed with special software (i.e. TOR)

Anonymizes traffic between a user and the target website

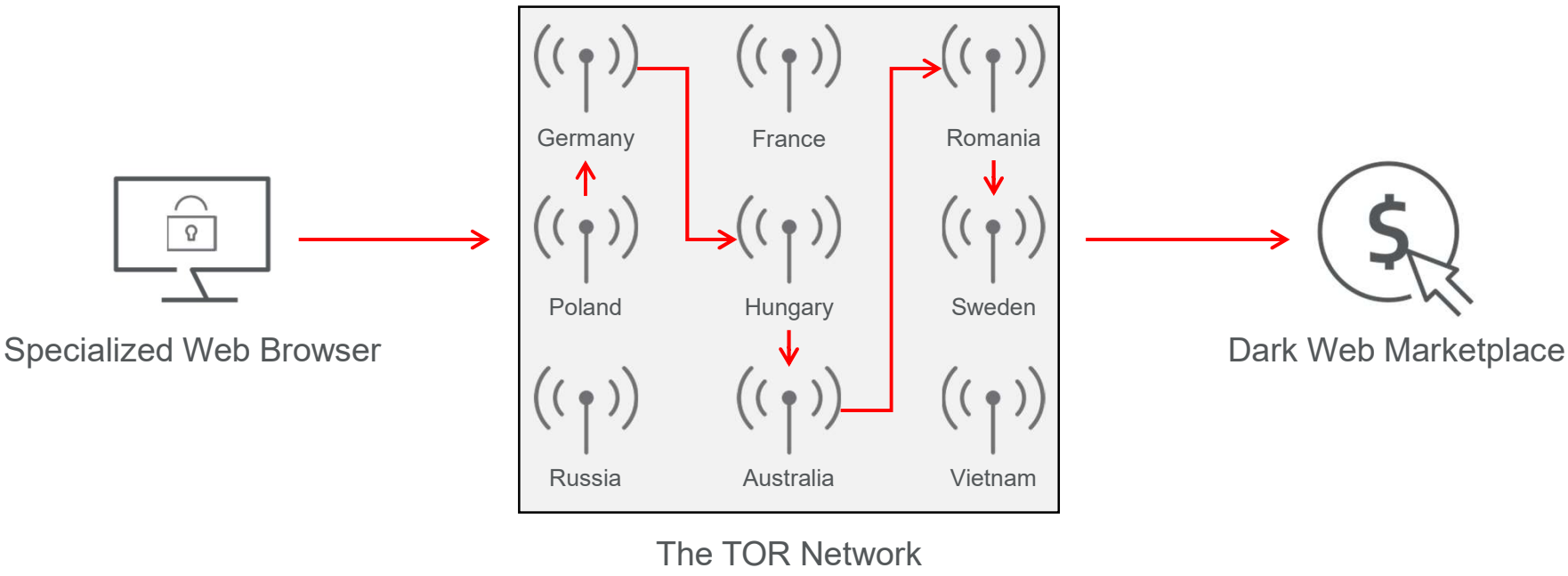
TOR originally developed by US Navy & DARPA

Used for sensitive networking



The Dark Web

TOR: The Onion Router



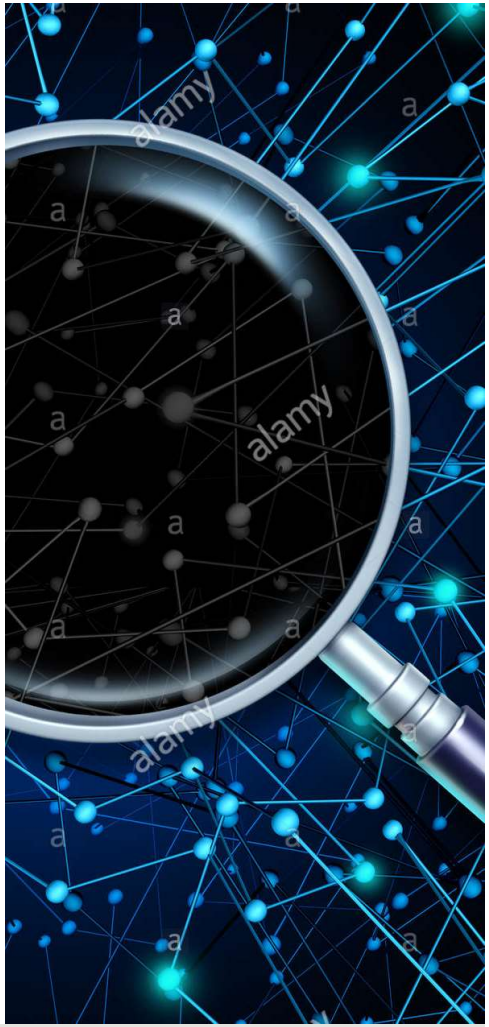
Misconceptions

The Dark Web is inherently neutral

A large percentage of content is benign

Many “Dark Web” and “Black Market” sites operate in the open Internet or Deep Web

Criminal activity traverses all layers of the Internet



Cybercrime: A Day in the Life

Criminal X runs spam and credential theft campaigns

Accidentally exposes their browser history

Slips up and down the “Internet Iceberg” sporadically

Cybercrime: A Day in the Life

09:00

Checks Gmail inbox
Checks Outlook inbox
Retrieves encrypted files
Logs into Malware dashboard
Reads over Malware reports
Logs into Dark Web “Forum A”

10:00

Logs into cybercrime “Forum B”
Forum B: reads thread about web injects
Forum A: reads thread about spam
Purchases a file encryption software
Checks bitcoin wallet balances
Files a support ticket with software vendor
Checks email for ticket number

11:00

Downloads clip art for spam campaign

12:00

Reads security blog on how to hide from AV
Forum A: reads a number of malware threads
Reads security blogs on famous hacking team

13:00

Forum A: reads new posts in spam thread
Reads Wikipedia articles about the term “0day”
Forum A: reads threads about getting past AV
Watches YouTube video about AV programs

14:00

Criminal X takes a siesta

Internet
Deep Web
Dark Web

Cybercrime: A Day in the Life

17:00

Forum A: reads threads about their Malware
Logs into spam email account(s)
Downloads more clip art for spam campaign
Forum B: reads ads for encryption services
Reads over Malware reports

18:00

Criminal X breaks for dinner

20:00

Forum A: reads new posts in spam thread
Forum A: reads threads about their Malware
Shops several different email services
Buys email service via secure payment
Buys several domains for hosting malware
Checks email for receipts / login information
Reads over Malware reports

21:00

Configures new malware domains
Looks into programming software

22:00

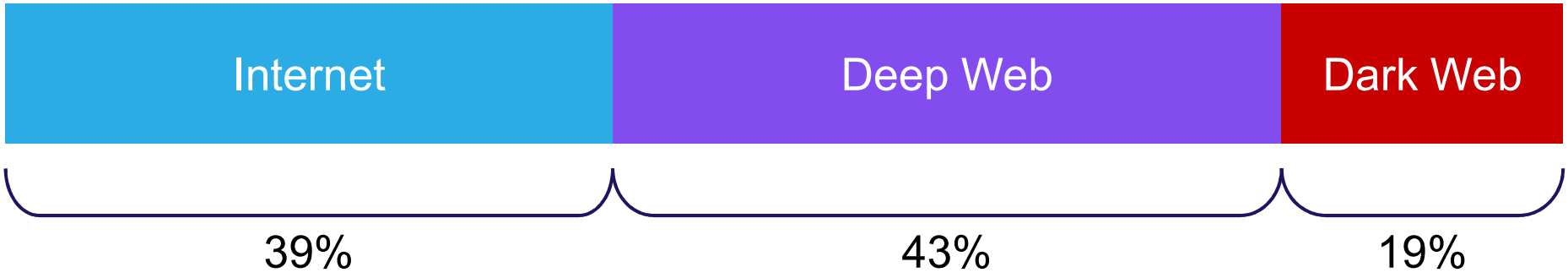
Browses several jewelry and clothing sites
Checks Gmail inbox one last time
Checks Outlook inbox one last time
Forum A: reads new posts and comments

23:00

Reads over Malware reports one last time
Criminal X heads to bed

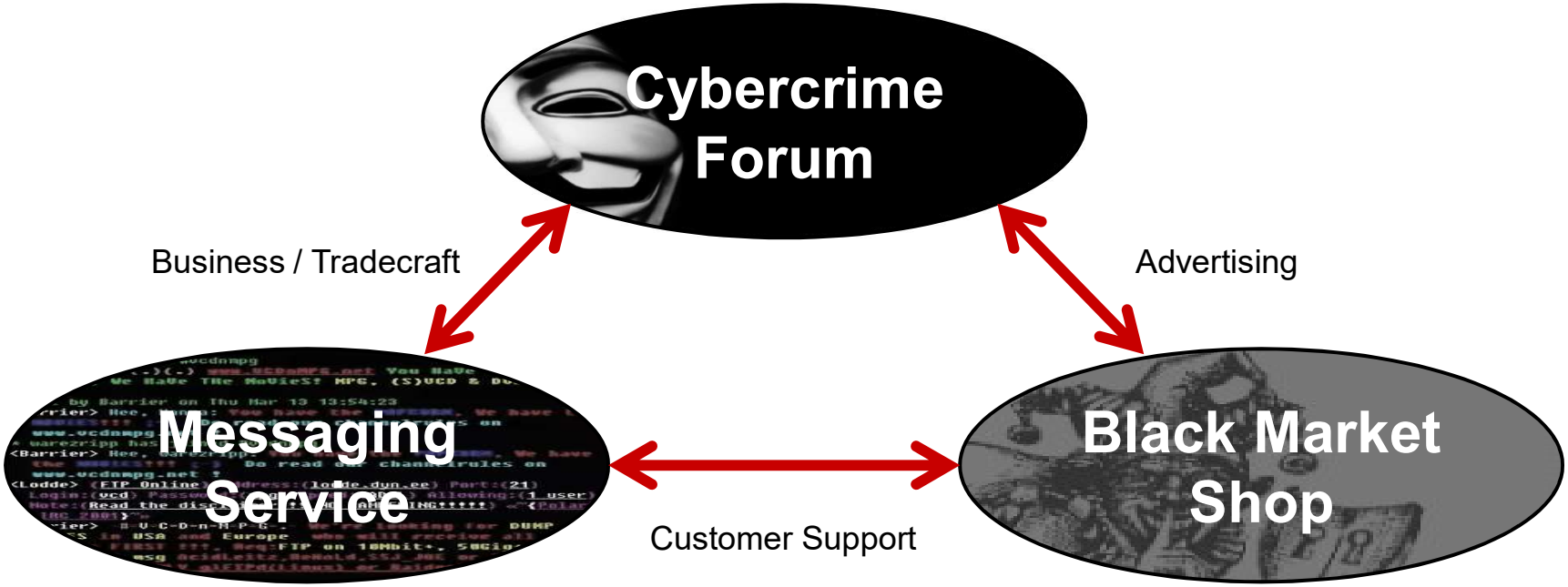
Internet
Deep Web
Dark Web

Cybercrime: A Day in the Life



OR

Underground Discourse



The Greater Value

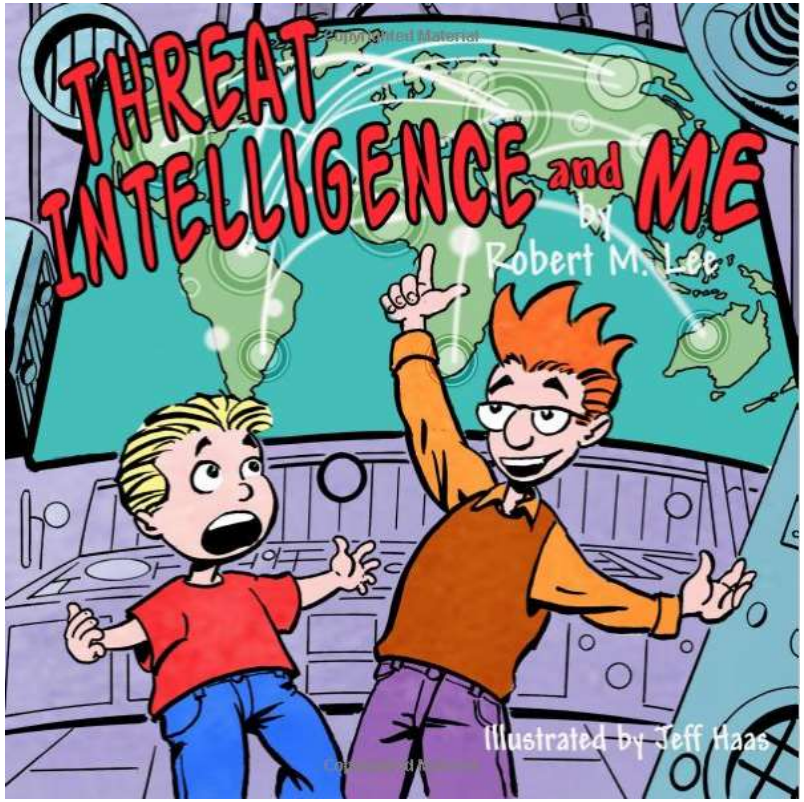
Criminal capability

Compromised assets and entities

Persona development and Identification

Shifting from Reactive to Proactive Measures

The Greater Value



The Greater Value

"Collecting intelligence is a hobby;
exploiting it is a profession."

-Robert M. Lee (SANS FOR578)