Something Dark

INVESTIGATING IN THE DARK WEB

CHAD LOS SCHUMACHER, ITHREAT CYBER GROUP

About iThreat Cyber Group

- Founded in 1997 in Princeton, New Jersey
- Provides Technology Enhanced Services
  - Investigative and monitoring services through iThreatFusion.center
- Offers Enhanced Data Services
  - Augmented and contextual answers to questions
- Licensed private investigations firm

About Chad Los Schumacher

- Manager, Technology Deployment at iThreat Cyber Group
- Masters of Science in Applied Intelligence from Mercyhurst University
- Bachelors of Science in Criminal Justice from Saint Leo University
- Provides training on DNS and investigations

Session Objectives

- Define what the dark web is
- Locate common hubs and key resources
- Introduce tools/methods for finding and/or unmasking dark web sites

Warning…

- The dark web is filled with some awful things that cannot be unseen
- Ask yourself if this is really the job for you before starting
- Review the risk/reward as it may create other headaches

Understanding the Parts of the Web

- **Surface web:** where most of your day-to-day activity takes place, sites visible to search engines.
- **Deep web:** Information that is more hidden or restricted, such as academic databases, newspaper archives, etc.
- **Dark Web:** Internet within an internet, designed to be anonymous and obfuscated

Uses for the Dark Web

FOR BETTER…

- To circumvent government censorship
- To provide whistleblowers protection
- To avoid monitoring

FOR WORSE…

- Enables sales of illegal firearms, drugs, counterfeits, etc.
- Human exploitation (porn, trafficking, etc).
- Hire hitmen, hackers, etc.

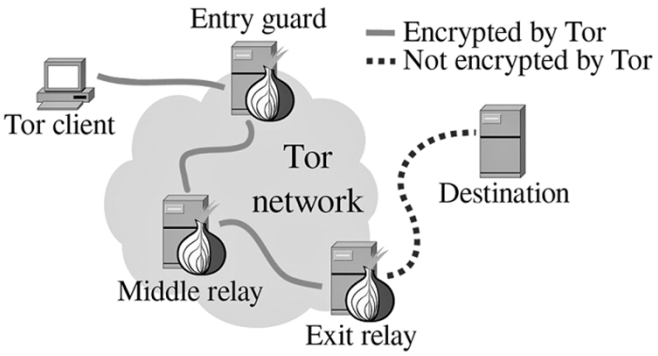
Differences Between the Dark Web and Open Web

- Requires special software to access, an Internet within an Internet
- Resistant to indexing, not easily searched
- Indices are similar to Yahoo! in 1995 (Directories vs. Search Engine)
- Communications within the network are *always* encrypted

Three Major Dark Webs

- The Onion Router (Tor) - Focus for this presentation
  - The biggest, most well known dark web.
  - Most Internet-like
- Invisible Internet Project (I2P)
  - Up and coming
  - Focuses on services (ie: instant messaging, email, websites, etc).
- Freenet
  - Distributed file sharing
  - Offers communications

How Tor Works



About .onion Sites

- Can only be accessed when using Tor
- No master database of all .onion sites
- Use of Tor allows for the creation of .onion sites
- Domains are randomly generated, either 16 or 56 characters long

Challenges with Tor Investigations

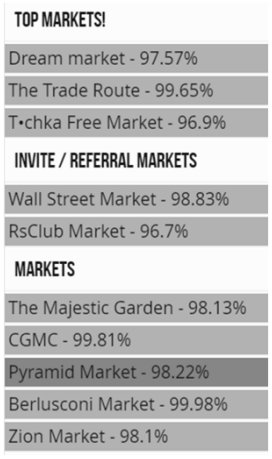
- The network was designed to provide anonymity
- Best chance at unmasking means finding a clear web connections
- They don't take PayPal, so be ready for Bitcoin
- Accounts need to be anonymized and not tied to your person
- There's no Google, so you may not find what you're after
- Cultural distrust of others

Where to Begin

LOCATING STARTING POINTS & ACCESSING

Google It!

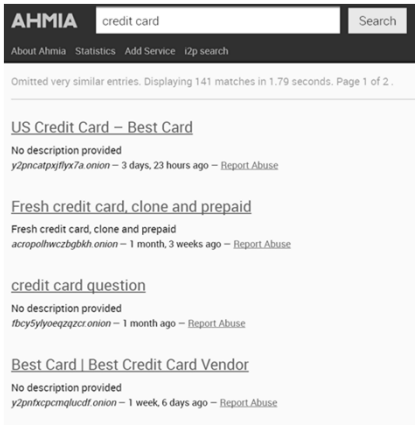
- Using Google/Bing provide excellent list of starting points
- Reddit, Twitter discuss dark web markets in open (r/deepweb)
- Dedicated sites in open web help new users find dark web markets (deepdotweb.com, darkwebnews.com)
- May have to get into deep web to find other markets



Deepdotweb.com

Searching the "Search Engines"

- Several Tor "search engines" exist that claim to scan/index Tor sites
- Each use their own techniques
- Nowhere near the power/sophistication of Google, Yahoo, etc
- Typically unreliable – data can be stale
- Biggest names: ahmia.fi and Torch Tor Search Engine



Other Lists/Resources

- Hunchly Daily Hidden Service
  - New .onions found daily by Justin Seitz at Hunchly – darkweb.hunch.ly
- Reddit
  - https://www.reddit.com/r/onions/search?q=url%3A.onion&sort=new&restrict_sr=on
- Paid services like Dark Owl, others

Going Dark: Two Fast Ways to Access

TOR BROWSER

- Developed by Tor Project
- Custom version of Firefox
- Provides plugins and tips to keep you anonymous
- **This is the best/safest option**

TOR2WEB GATEWAYS

- Add .to, .casa, .direct, or .rip to access Onion sites directly
- These are often run by individuals or organizations
- It is unclear what some are doing with the data (especially .link)
- **Use with caution!**
- Ex: facebookcorewwwi.onion.to

Bringing the Dark to the Light

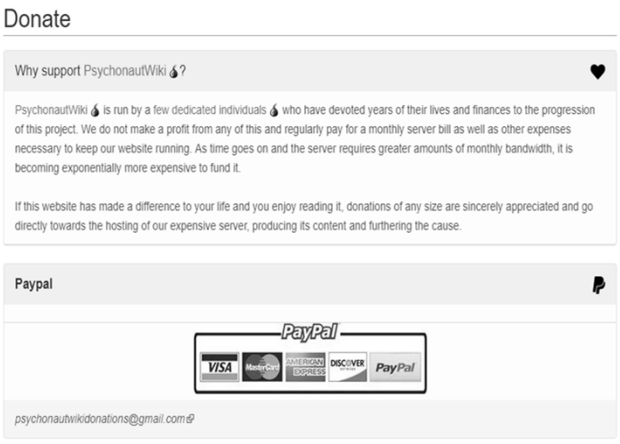
TECHNIQUES AND TOOLS

Look for the Obvious: Clear Web Mentions

- Do you see any of the following referenced?
  - A clear web domain (example.com, example.net, etc)
  - A social media account like Facebook or Twitter
  - A clear web email (Gmail, Hotmail, or other custom domain)
  - Payment methods like PayPal, Venmo, Zelle, etc.
- Right click on the page and select "View Page Source"
  - Search the page for .com, .net, @gmail.com, etc for potential hidden links
  - Webmasters may make mistakes and point to a clear web domain instead of a .onion

These data points are present more often than you think!

Examples of Clear Web Connections

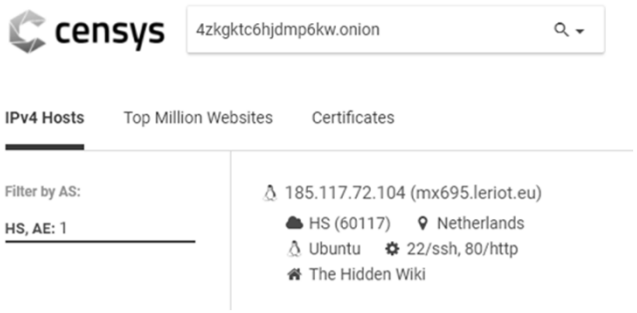


psychonaut3z5aoz.onion

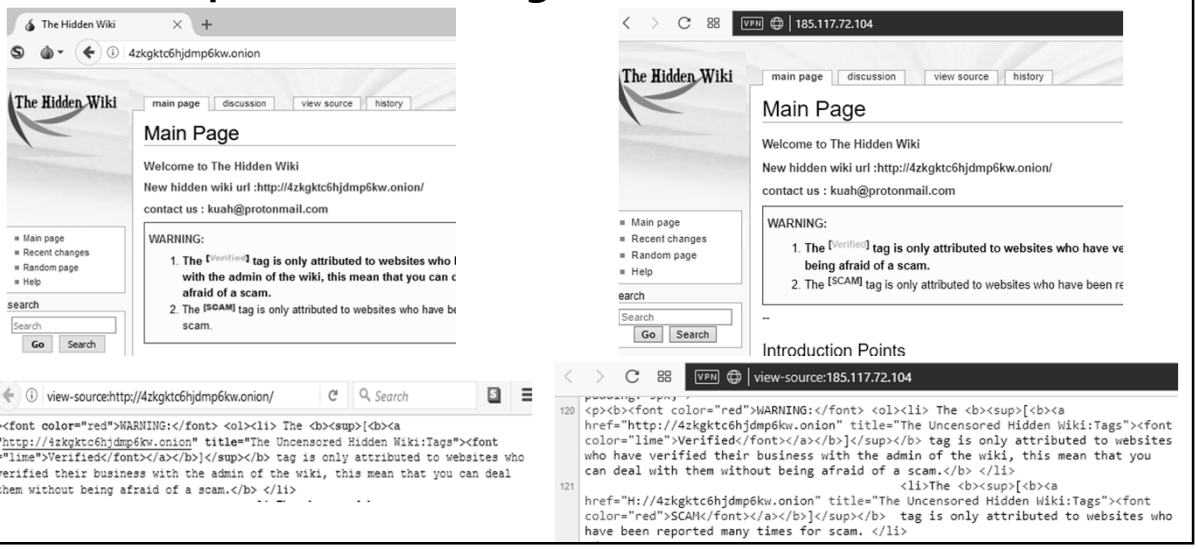
a9a19b3635191ebe97b9d3f61addc93a.endchan5doxvprs5.onion

Possible Leaking IP Address with Censys.io

- Service scans IP address space for running services and makes it searchable by domain or IP address
- Entering a .onion can return an IP if a server is misconfigured



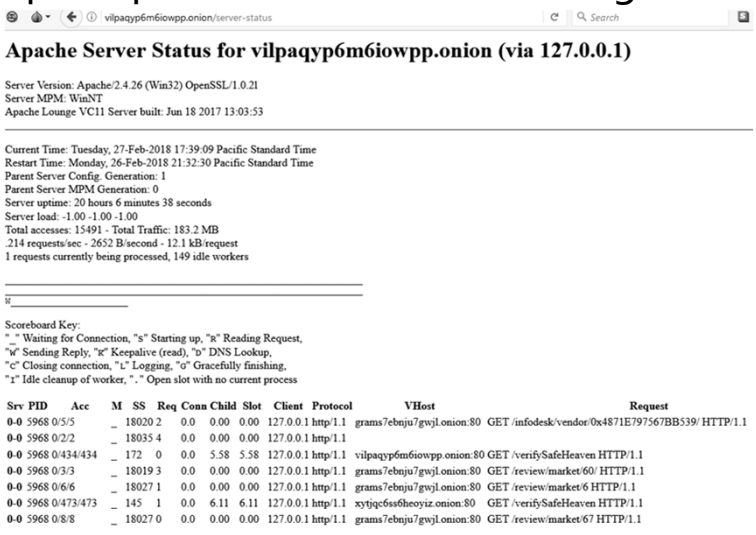
Example of a Leaking .onion



Check for Sites on the Same Server

- Only works for sites running Apache web server.
- Visiting example.onion/server-status can reveal:
  - Server information (operating system, uptime status, creation date)
  - Other domains using the same server
  - IP addresses accessing the server
  - What resources (pages, images, etc) are being accessed

Example Apache Server Status Page



vilpaqyp6m6iowpp.onion/server-status

Apache Server Status for vilpaqyp6m6iowpp.onion (via 127.0.0.1)

Server Version: Apache/2.4.26 (Win32) OpenSSL/1.0.2l
Server MPM: WinNT
Apache Lounge VC11 Server built: Jun 18 2017 13:03:53

Current Time: Tuesday, 27-Feb-2018 17:39:09 Pacific Standard Time
Restart Time: Monday, 26-Feb-2018 21:32:30 Pacific Standard Time
Parent Server Config. Generation: 1
Parent Server MPM Generation: 0
Server uptime: 20 hours 6 minutes 38 seconds
Server load: -1.00 -1.00 -1.00
Total accesses: 15491 - Total Traffic: 183.2 MB
.214 requests/sec - 2652 B/second - 12.1 kB/request
1 requests currently being processed, 149 idle workers

Scoreboard Key:
"_" Waiting for Connection, "s" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M	SS	Req	Conn	Child	Slot	Client	Protocol	VHost	Request
0-0	5968	0/5/5	_	18020	2	0.0	0.00	0.00	127.0.0.1	http/1.1	grams7ebnju7gwjl.onion:80	GET /infodesk/vendor/0x4871E797567BB539/ HTTP/1.1
0-0	5968	0/2/2	_	18035	4	0.0	0.00	0.00	127.0.0.1	http/1.1		
0-0	5968	0/434/434	_	172	0	0.0	5.58	5.58	127.0.0.1	http/1.1	vilpaqyp6m6iowpp.onion:80	GET /verifySafeHeaven HTTP/1.1
0-0	5968	0/3/3	_	18019	3	0.0	0.00	0.00	127.0.0.1	http/1.1	grams7ebnju7gwjl.onion:80	GET /review/market/60/ HTTP/1.1
0-0	5968	0/6/6	_	18027	1	0.0	0.00	0.00	127.0.0.1	http/1.1	grams7ebnju7gwjl.onion:80	GET /review/market/6 HTTP/1.1
0-0	5968	0/473/473	_	145	1	0.0	6.11	6.11	127.0.0.1	http/1.1	xytjqc6ss6heoyiz.onion:80	GET /verifySafeHeaven HTTP/1.1
0-0	5968	0/8/8	_	18027	0	0.0	0.00	0.00	127.0.0.1	http/1.1	grams7ebnju7gwjl.onion:80	GET /review/market/67 HTTP/1.1

In Conclusion

- Covered definitions of the dark web, how Tor works
- Reviewed where to find dark web sites and resources
- Provided resources and ways to potentially de-anonymize a .onion

Question? Comments?

CHAD LOS SCHUMACHER
@ITISJUSTCHAD
CLS@ICGINC.COM
+1 609 806 5000