Welcome to the (Sock) Jungle
Who Am I?

Craft beer geek, Peathead, Crossfit enthusiast, Ultimate Frisbee freak

Lead Consultant, Ensign InfoSecurity
» Lead the team in conducting CTI operations
» Develop collection capabilities for the team

Intelligence Officer, Singapore Armed Forces
» 9 years conducting military intelligence operations
» 1 year conducting web intelligence for counter-terrorism operations
What I Needed To Do To Create Sock Puppets

» Use a VM (e.g. VMware, Virtualbox)
» Have an email to sign up for stuff
» Pay anonymously
» Staying anonymous in general
» Access social media accounts without getting the verification screen
» Have a bunch of untraceable stuff:
  • Email
  • Fake Particulars
  • Temporary phone numbers
» Keeping track of multiple sock puppets
Being Contactable

Email and SMS
Being Contactable (for email verification)

» Email is the basic requirement as it’ll be needed for account registrations

» Surface Web Email Providers
  • Protonmail - http://www.protonmail.com
  • Tutanota - http://www.tutanota.com

» Dark Web Email Providers
  • Secmail Tor - http://secmailw453j7piv.onion
  • Mail2Tor - http://mail2tor2zyjdctd.onion

» Email Masking
  • Used to quickly generate email addresses to register multiple accounts on a single site
  • Blur - https://abine.com
Being Contactable (for SMS verification)

» Large number of sites require SMS verification during registration
  • Long code vs short code

» Various ways of dealing with this:
  • Prepaid SIM cards (best way)
  • Virtual Numbers (free & paid)
  • SMS verification sites

» Paid Providers
  • Mint Mobile
  • Twilio - https://www.twilio.com

» Free Providers
  • TextNow - https://www.textnow.com/
  • Talkatone - https://www.talkatone.com/
Devil is in the Details
The Devil is in the Details

» Basic details that you need for your sock puppet:
  • Name
  • Age
  • Birthdate
  • Address
  • Sex
  • Phone number

» Other details you might need:
  • Credit Card
  • Social Security No.
  • Browser User Agent

» Fake Name Generator is a great tool to start off
  • Bulk identity generator
  • https://www.fakenamegenerator.com/
How much Details?

» For **passive collection**, just need to have enough details to get past verification
  • Mass create and harvest away

» **Active Engagement**
  • Hacking forums/groups
    • Does not matter if you have a believable background because everyone is using sock puppets
How much Details?

» Active Engagement
  • Non-cyber Targets
    • Create a believable backstory but don’t stand out too much
    • Make sure all your social media accounts are created in the ‘correct’ locations and posts are made in the correct time zone
  • Ensure that your pictures cannot be found using reverse image search
  • Dox your own sock puppet before deploying for engagement
Paying the Bills

It’s all about the money
Paying the Bills (BTC)

» Bitcoins (BTC) were used for paying most online services

Ways of getting BTC:

» Coin Exchanges
  • Convenient but it needs personal particulars as it is a regulated financial institute (in Singapore)
  • BTCs can be cleaned up using BTC tumbling services like https://bitcoin-laundry.com/
Paying the Bills (BTC)

» BTC ATM
• No personal particulars needed and BTCs are bought with cash
• Need to physically locate ATMs - https://coinatmradar.com/

» Using Gift Cards
• Generally bad exchange rates, great if you had loads of free gift cards lying around, which is not shady at all...
• https://paxful.com/buy-bitcoin
Paying the Bills (Others)

» Prepaid debit cards
  • Only cards that cannot be reloaded should be used as they don’t require any personal information
  • OneVanilla Prepaid Visa Card
    • https://onevanilla.com/
Staying Anonymous
Staying Anonymous

» Anonymity vs Privacy
   • **Anonymity**
     • People can see what you’re doing but don’t know who you are
     • Sock puppets, TOR, bitcoin transactions
   • **Privacy**
     • People know who you are but don’t know what you’re doing
     • VPN, private social media accounts

• Use VPNs and proxies
Don’t Be Cheap!

» Do not use free VPNs or Proxies
  • Log connections
  • Monitor users’ browser habits
  • Sell customer data to advertisers
  • Spying on customer traffic

» Paid services offer:
  • Better connection speeds
  • Guaranteed uptime
  • Privacy policies
  • Multiple locations
Considerations for Buying VPN Services

» No logging policy

» Offers payments methods such as cryptocurrencies or gift cards
  • No personal information is required during registration

» Companies that don’t reside in any of the countries in 5, 9 or 14 Eyes

<table>
<thead>
<tr>
<th>Five Eyes</th>
<th>Nine Eyes</th>
<th>Fourteen Eyes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Australia</td>
<td>1. Denmark</td>
<td>1. Belgium</td>
</tr>
<tr>
<td>2. Canada</td>
<td>2. France</td>
<td>2. Germany</td>
</tr>
<tr>
<td>3. New Zealand</td>
<td>3. Netherlands</td>
<td>3. Italy</td>
</tr>
<tr>
<td>5. United States of America</td>
<td></td>
<td>5. Sweden</td>
</tr>
</tbody>
</table>

Source: https://thatoneprivacysite.net/#detailed-vpn-comparison
Building a Disposable VPN

» AlgoVPN - https://github.com/trailofbits/algo

» Buy VPS service from companies that accept cryptocurrencies
  • Bitlaunch.io, coinshost.com, etc

» Pros
  • Speed guaranteed as there is only one user
  • Can destroy VPN after use
  • No logging of traffic by the server
  • Sets up in around 15 mins

» Cons
  • Only a single IP address available
  • Requires some technical knowledge to set up
# Residential/Mobile IP VPNs/Proxies

**ISP:** Web2Objects LLC  
**Host Name:** 45.56.153.218  
**ASN:** 22400

<table>
<thead>
<tr>
<th>IP Address</th>
<th>50.239.137.202</th>
</tr>
</thead>
<tbody>
<tr>
<td>City</td>
<td>Capitol Heights</td>
</tr>
<tr>
<td>State/Region</td>
<td>Maryland</td>
</tr>
<tr>
<td>Country Code</td>
<td>United States</td>
</tr>
<tr>
<td>Postal Code</td>
<td>20731</td>
</tr>
<tr>
<td>ISP</td>
<td>Comcast Cable Communications LLC</td>
</tr>
</tbody>
</table>

## Regular VPN/Proxies

## Residential/Mobile IP VPN/Proxies
Mobile IP Proxy “Rack”
Getting Your Browser Ready
Getting Your Browser Ready

AdBlock Plus
Blocks ads and disables trackers

Privacy Badger
Disables trackers on websites

SwitchyOmega
Routes browser traffic through a proxy server

UserAgent Switch
Spoofs user agent of browser

Blur
Provides masked emails and password manager

Cookie Auto Delete
Auto deletes cookies when tabs close

Edit This Cookie
Copy or paste cookies from websites

Tracker Management
Deleting of trackers will reduce the chances of browser being fingerprinted

Sock Management
Helps to manage multiple sock puppets including IP location and user agents

Cookie Management
Ensures that cookies are not stored and managed saved cookies for logins
And we are ready to create some accounts!
Creating Social Media Profiles

» Major social media platforms are connected to each other
» Facebook is the most important platform to start off first
Tips on Social Media Avatars

» Cultivating an avatar takes time (about 3 - 6 months)

» Don’t do things that you wouldn’t do for your own account
  • Request to join 20 groups in a span of 10 mins
  • Randomly adding 10 people that are in a group that you’ve just joined as friends

» Do human-like things
  • Cultivate hobbies for your avatars
  • Occasionally like posts from your hobby groups/pages
  • Play games or watch cat/dog videos
In a Nutshell…

Being Contactable ➔ Personal Details ➔ Paying your bills

Sign Up Accounts ➔ Getting your browser ready ➔ Anonymity
Thank You

Zhuang Weiliang (Will)

@egomy_cs