Tor Network

Objectives

- What is Tor Network
- How Tor network works
- Web layers
- How a Tor hidden service works
- Tor vs. VPN

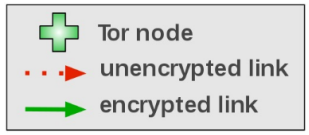
Tor Network

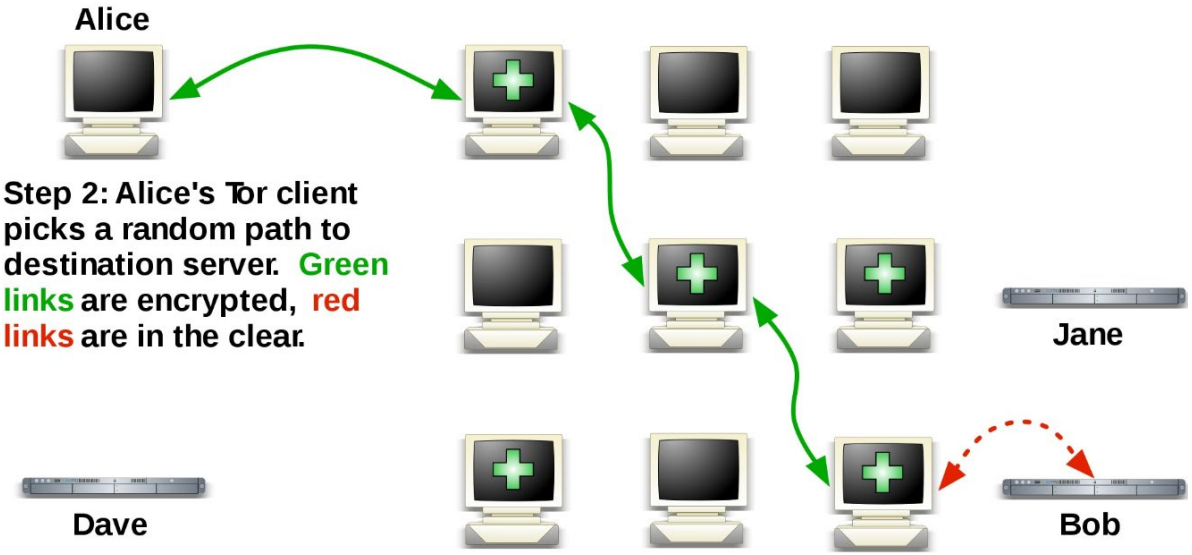
- The Tor Browser is a web browser that anonymizes your web traffic using the Tor network, making it easy to protect your identity online.

- Tor Browser is free and open-source software … Tor project

https://www.torproject.org/

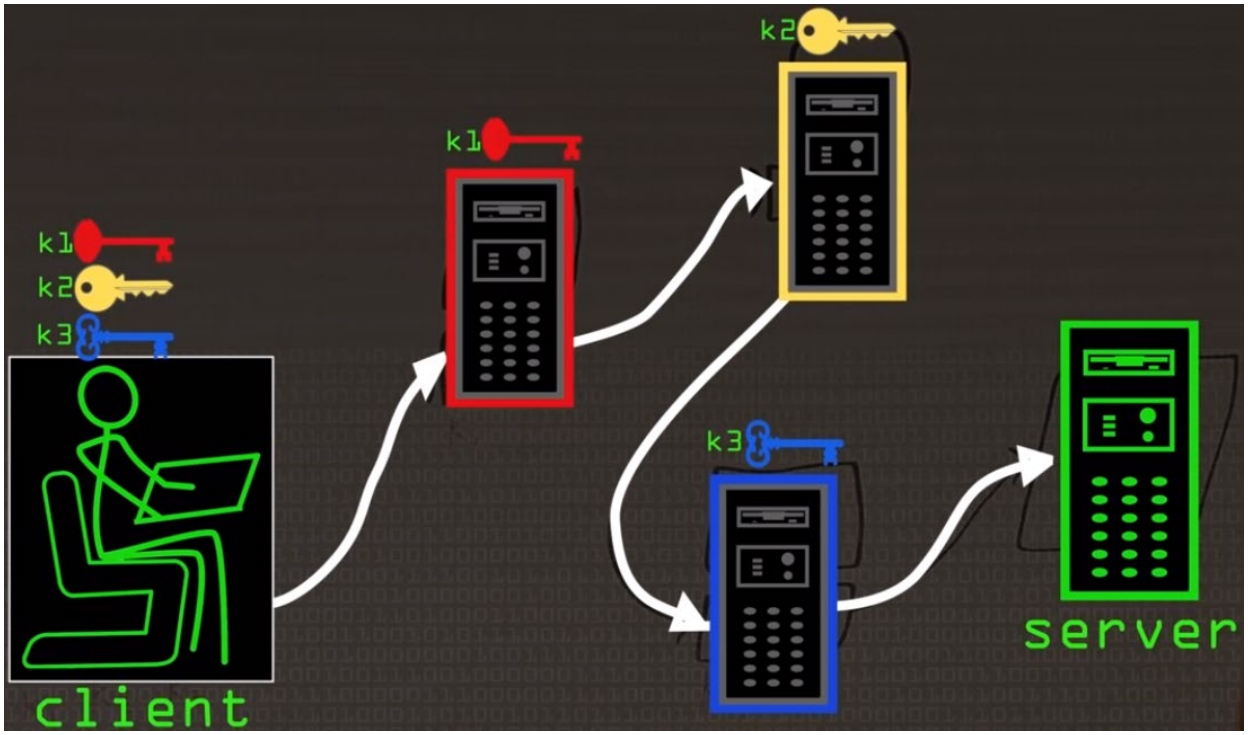
How Tor Network Works

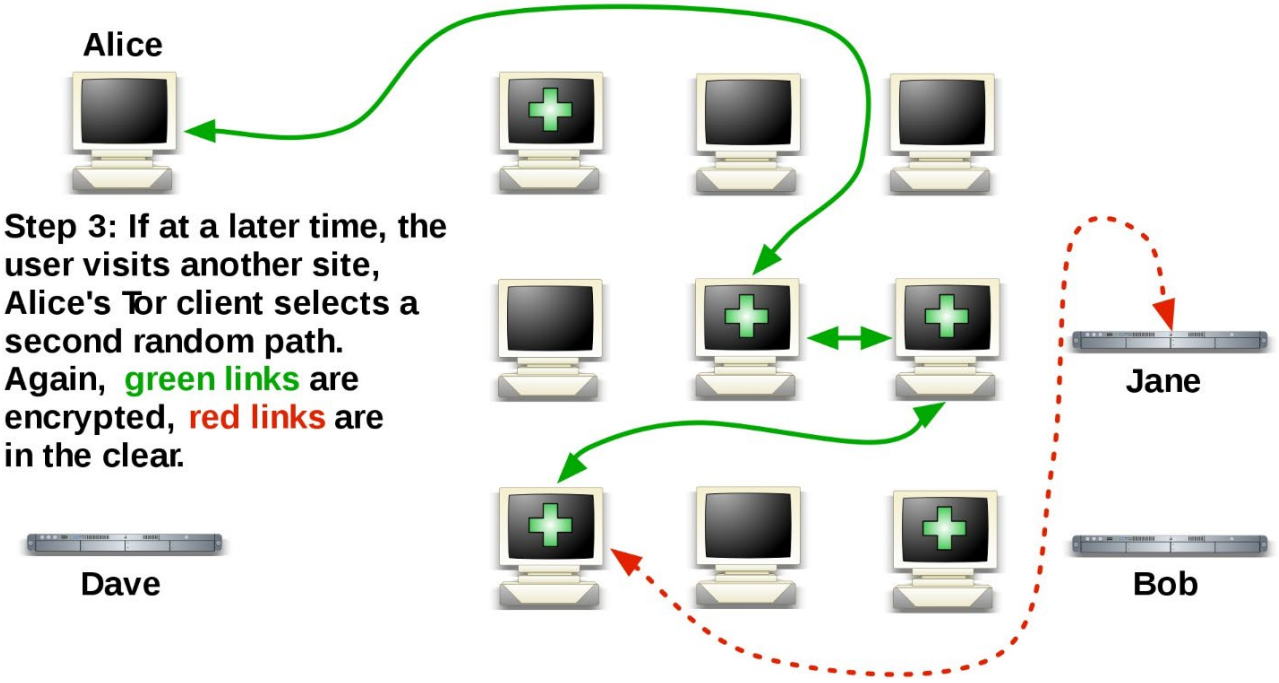




https://2019.www.torproject.org/docs/onion-services

- Every node is assigned a key before communication starts – allowing decryption of the outer layer before passing to the next node.
- Onion routing sends messages encrypted multiple times with different keys in layers



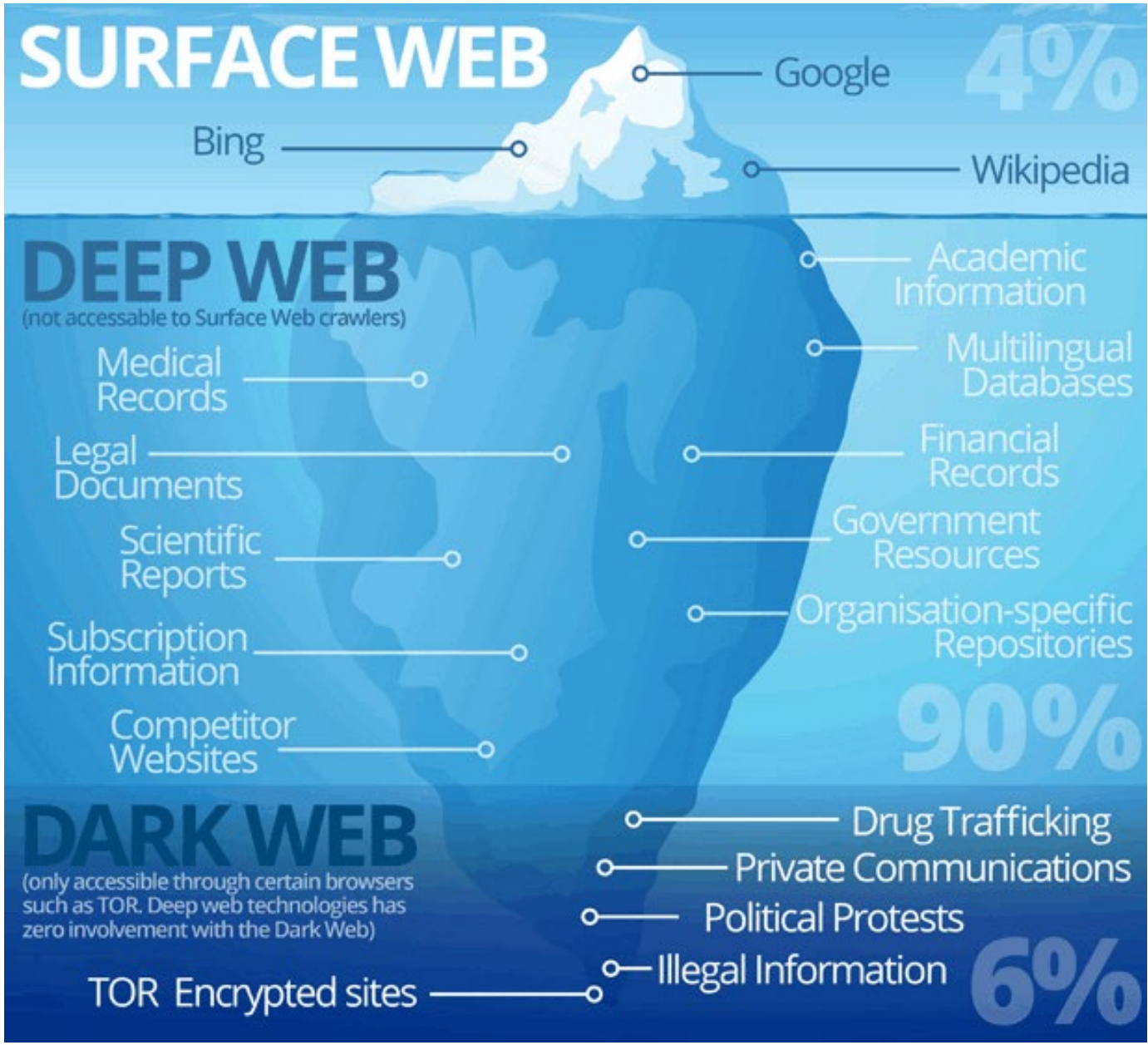


- What if the guard and exit nodes know each other

https://2019.www.torproject.org/docs/onion-services

Web Layers

- Surface web
- Deep web
- Dark web



The Surface Web

- Also known as the ’visible Web’ or ‘indexed web’
- Available to the general public
- Searchable with standard web search engines (e.g. Google, Yahoo, etc.)
- Content is indexed by search engines
- Little illegal activity
- Relatively small in size … estimated 4-10%

The Deep Web

- Also known as “invisible web” or ”hidden web”
- Not indexed by standard web search engines
- The content of the deep web can be located and accessed by a direct URL or IP address
- Accessible by password, encryption, or through gateway software
- Huge in size and growing exponentially … estimated 90%

The Dark Web

- Not indexed by standard web search engines
- .onion sites
- Have to have Tor installed and running to access .onion sites
- Intentionally hidden
- Large scale illegal activity
- Unmeasurable due to nature … expected 6-10%

Silk Road

anonymous market

messages 1 | orders 0 | account ฿0.00

Search Go

a few words from the Dread Pirate Roberts

Hi, [redacted] logout

0

Shop by Category

- Drugs *4,093*
  - Cannabis *999*
  - Dissociatives *78*
  - Ecstasy *314*
  - Opioids *354*
  - Other *153*
  - Precursors *18*
  - Prescription *903*
  - Psychedelics *586*
  - Stimulants *390*
- Apparel *82*
- Art *5*
- Books *768*
- Collectibles *15*
- Computer equipment *42*
- Custom Orders *27*
- Digital goods *369*
- Drug paraphernalia *153*
- Electronics *35*
- Erotica *296*
- Fireworks *5*
- Food *4*
- Forgeries *55*
- Hardware *1*
- Herbs & Supplements *11*
- Home & Garden *6*
- Jewelry *57*

5G Cocaine Pure Cistal Flakes
฿41.94

[28.0G] High Quality Crystal Meth
฿188.72

>>SPECIAL OFFER " BRAND SUBOXONE
฿0.91

alprazolam [Xanax] 100 x 1mg
฿11.31

Cocaine of high quality over 80% purity 25 gram
฿190.12

Ethyphenidate -2,5g- of the best racemic HCl qlt
฿6.18

Colombian Cocaine Lady´s and Gentleman 10G
฿67.32

0.5g #3 Brown Heroin , good quality!
฿7.52

News

- Closing the Armory
- A brand new look for Silk Road!
- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes

Products | Login | Register | FAQs

UK Passports

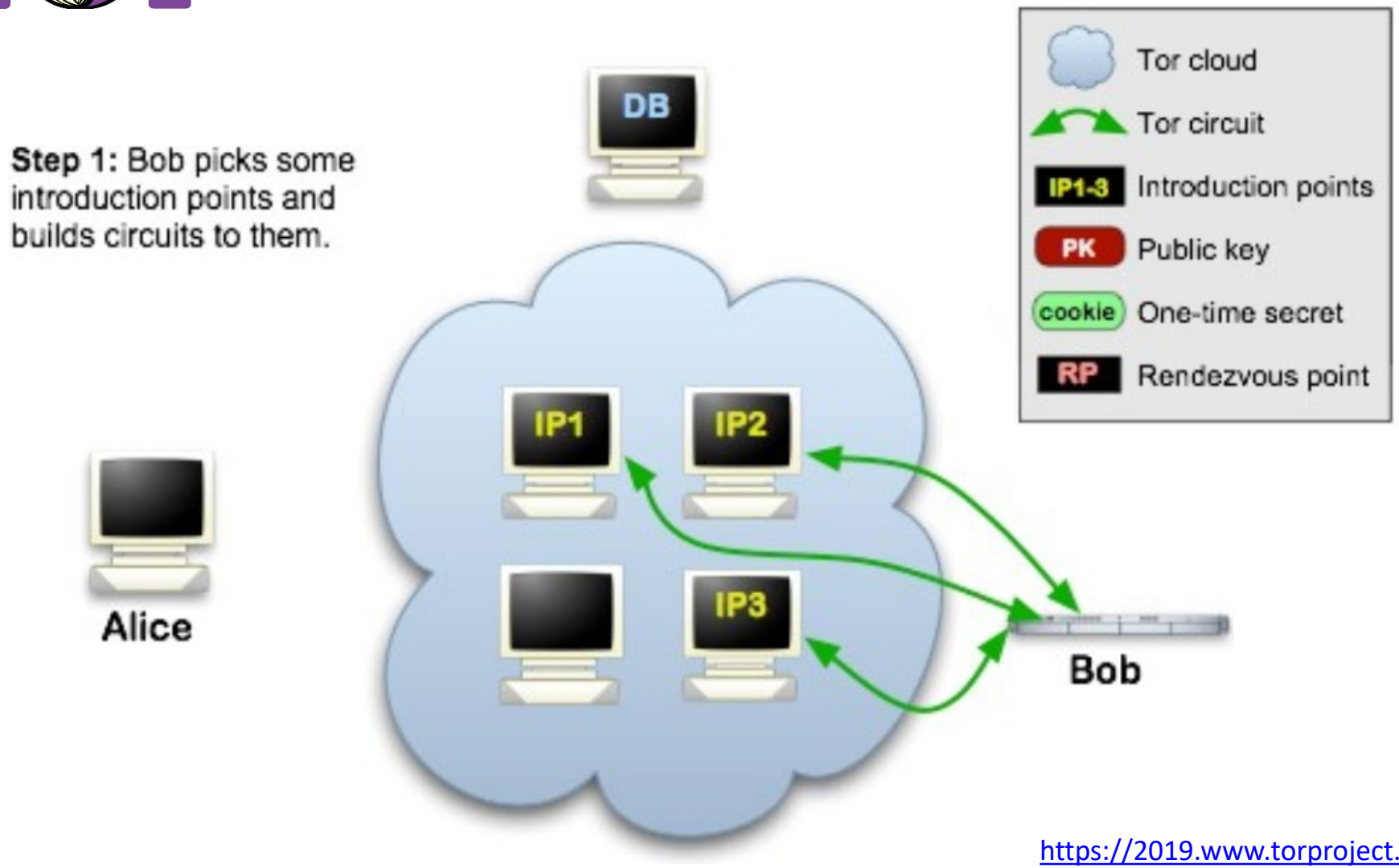
Your UK Passport - Name of your choice!

We are selling original UK Passports made with your info/picture.
Your info will get entered into the official passport database.
So it's possible to travel with our passports.
How we do it? Trade secret!
Information on how to send us your information and pictures will be given after purchase!

You can even enter the UK/EU with our passports, we will add a stamp for the country you are in before we send you your passport to any country!
Ideal for people who want to work in the EU/UK.

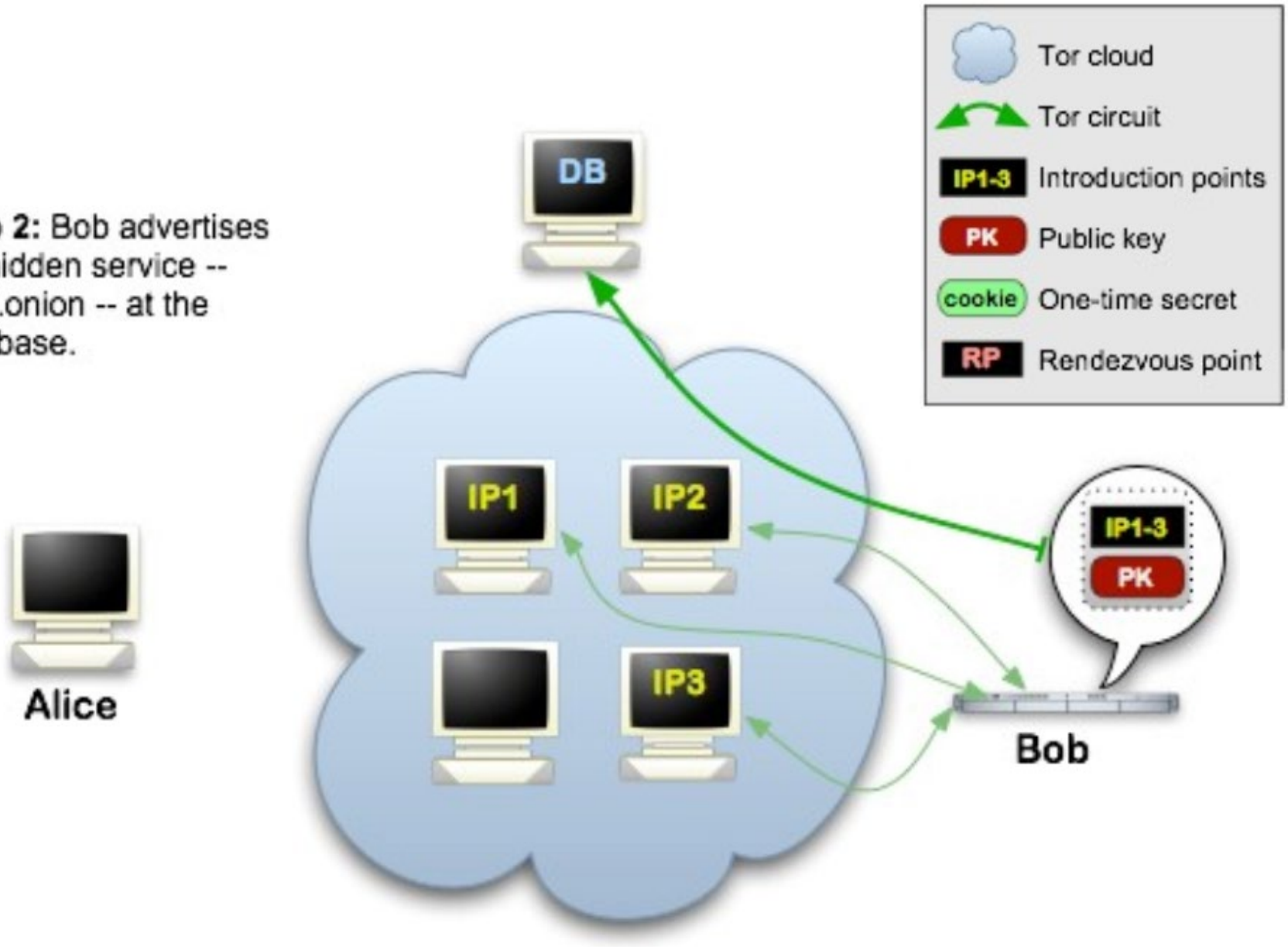
Product	Price	Quantity
Your original UK passport with your info/pictures This is 50% of the final price, you pay the other 50% once we show you pictures of your new passport	1000 GBP = 0.228 ฿	1 X Buy now
NEW: UK bank account with online banking and card. Great for cashing out bitcoin. Accounts are created in a secure way to make sure they don't get banned.	700 GBP = 0.160 ฿	1 X Buy now

How A Tor Hidden Service Works

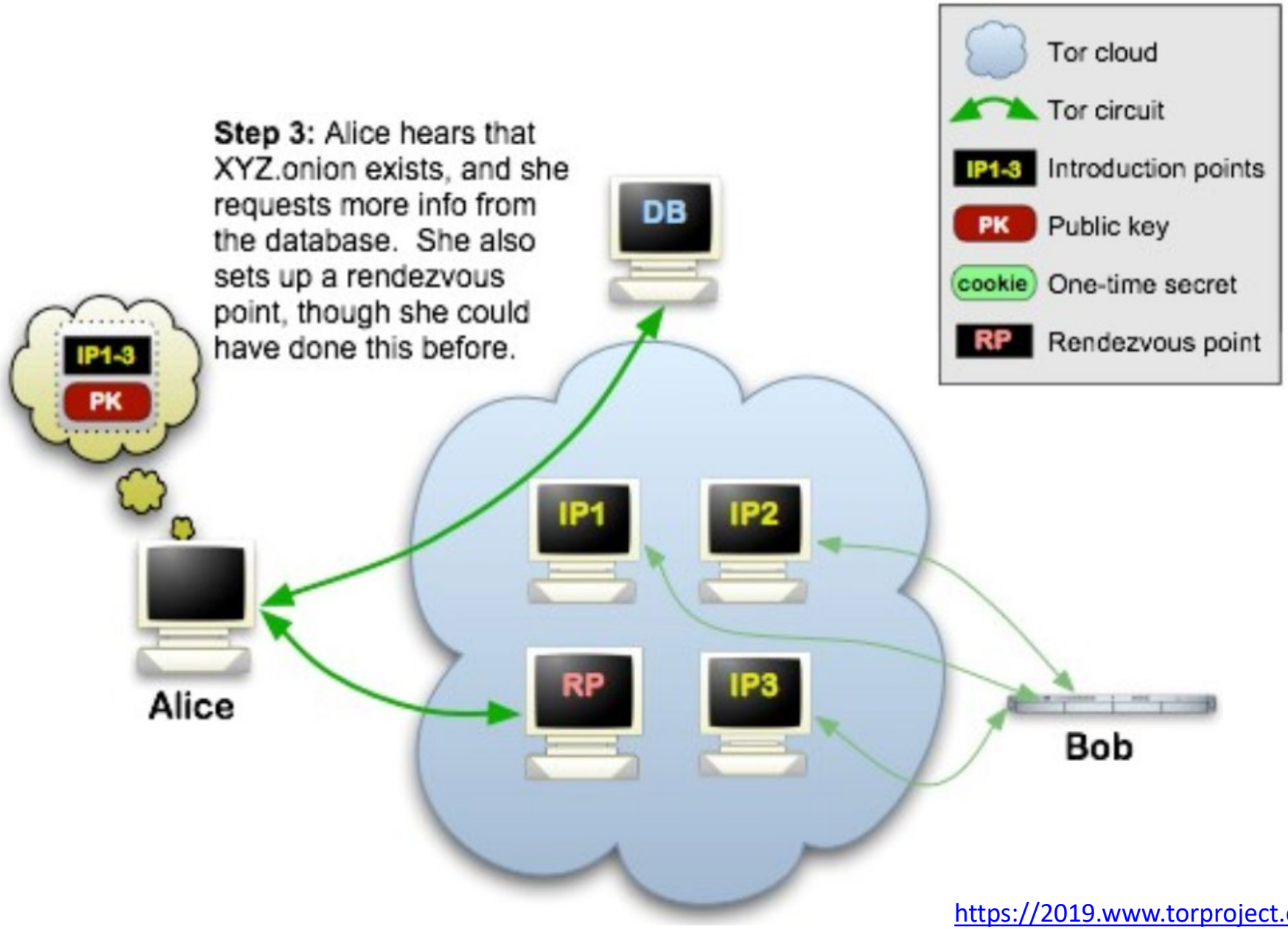


https://2019.www.torproject.org/docs/onion-services

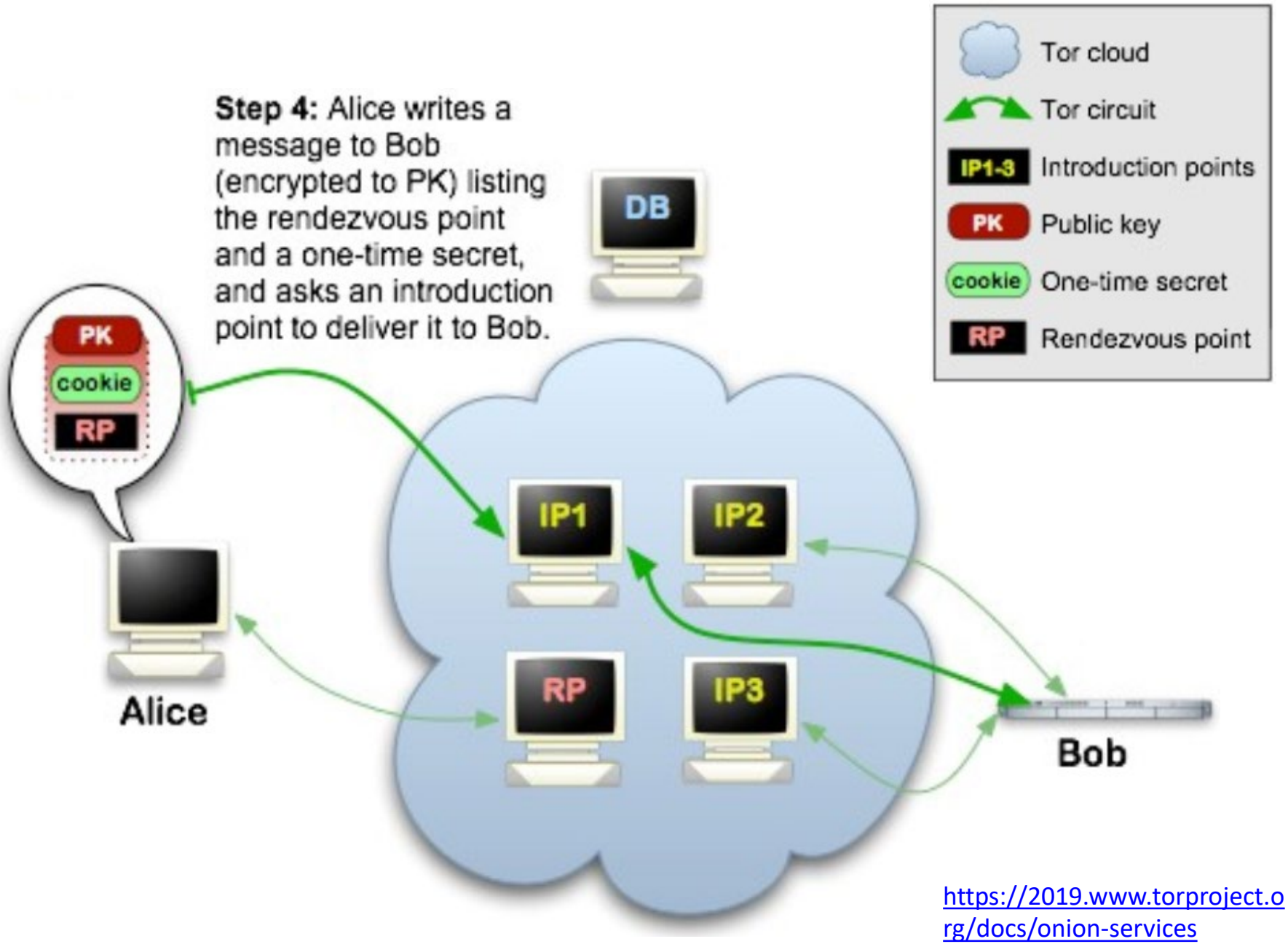
Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.



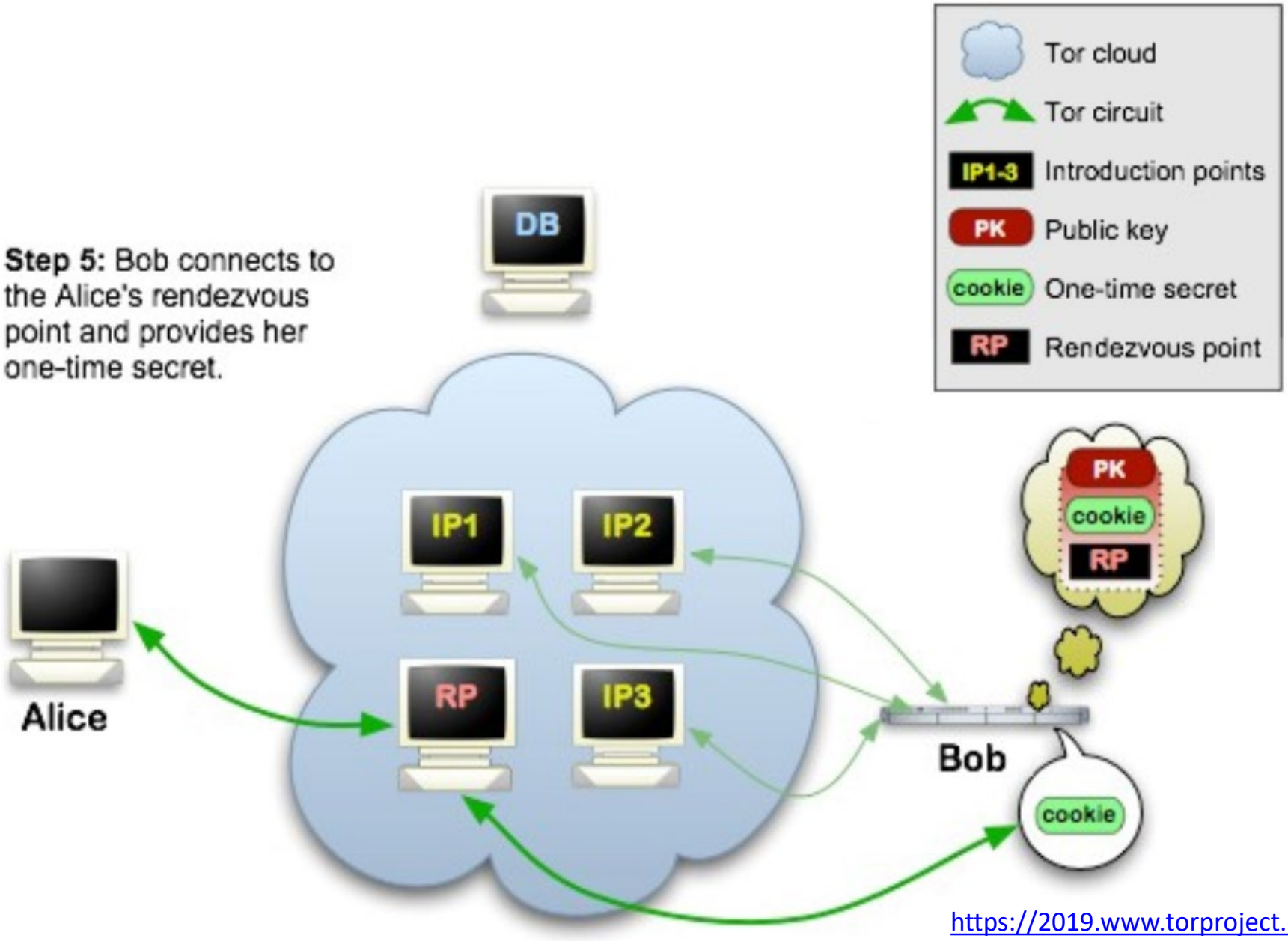
https://2019.www.torproject.org/docs/onion-services



https://2019.www.torproject.org/docs/onion-services



https://2019.www.torproject.org/docs/onion-services



https://2019.www.torproject.org/docs/onion-services

Tor vs VPN

- Both are used for anonymizing your network connections and encrypting them

- Tor pros:
  - Free
  - Best anonymity
- Tor cons:
  - Slow
  - Some websites might not work
  - Tor might not be available
  - Tor exit nodes can eavesdrop on communications
  - Doesn’t protect all applications

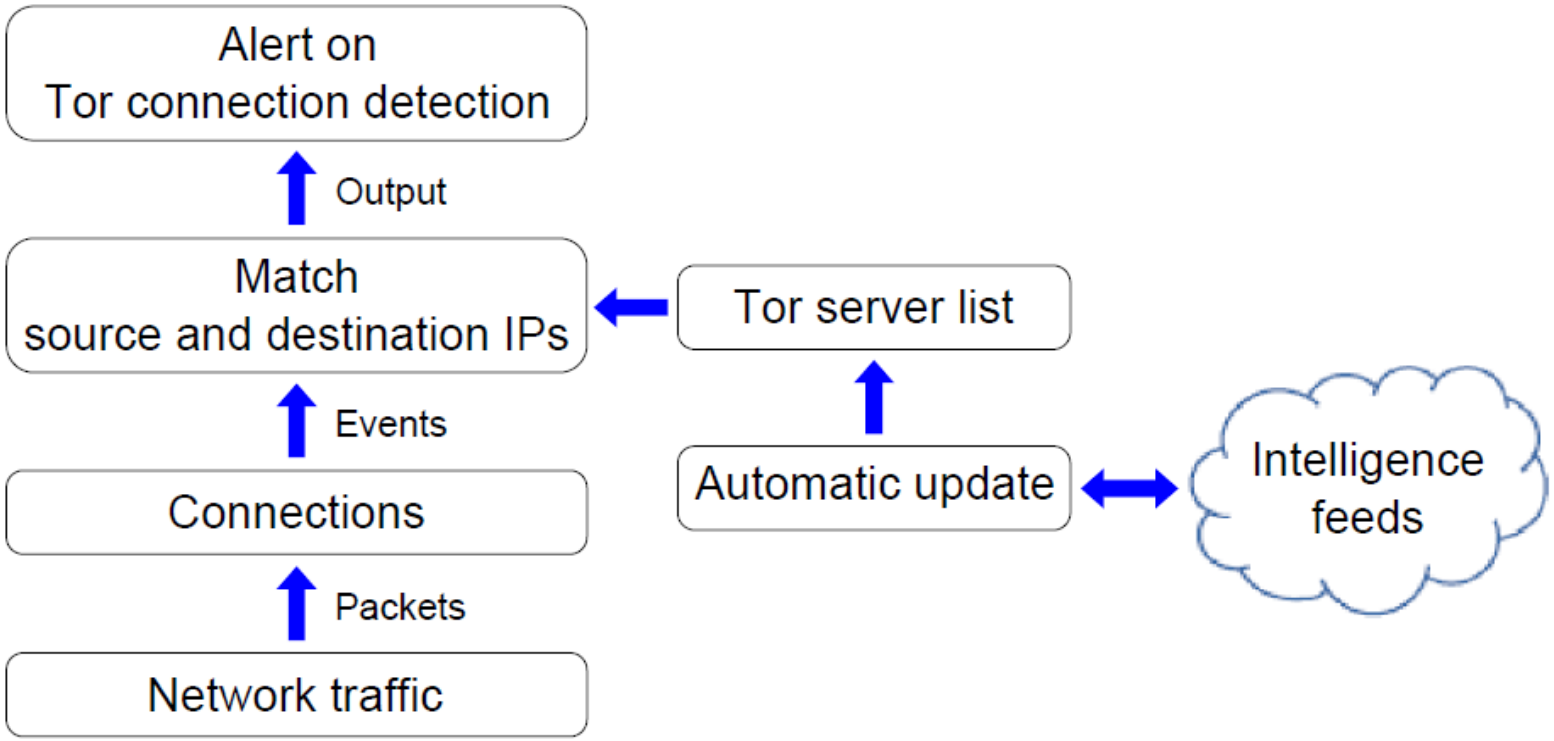
- VPN pros:
  - Faster
  - Most websites will work
  - Can pick location
  - Great at protecting public WiFi
  - Protects all applications
- VPN cons:
  - Not free (at least the good ones)
  - Privacy not as good as Tor

Tor Connection Detection (TorCD)

Algorithm 8 Implementation pseudo-code of TorCD

```
1: Get Tor servers list (t_tor_server table)
2: Get connection_established event
3: Check if the connection is to a Tor network:
4: if the connection destination IP is in t_tor_server then
5:     if the connection source IP belongs to the monitored network
6:         then
7:         if the same tor_alert has been generated over the last day
8:             then
9:             goto Check if the connection is from a Tor network:
10:        else
11:            Generate an event (tor_alert)
12:            Write tor_alert into tor_detection.log
13:            Send an alert email to RT
14:            Suppress the same tor_alert over the next day
15:        end if
16:    else
17:        goto Check if the connection is from a Tor network:
18:    end if
19: else
20:    goto Check if the connection is from a Tor network:
21: end if
22: Check if the connection is from a Tor network:
23: if the connection source IP is in t_tor_server then
24:    if the connection destination IP belongs to the monitored
25:        network then
26:        if the same tor_alert has been generated over the last day
27:            then
28:            goto End
29:        else
30:            Generate an event (tor_alert)
31:            Write tor_alert into tor_detection.log
32:            Send an alert email to RT
33:            Suppress the same tor_alert over the next day
34:        end if
35:    else
36:        goto End
37:    end if
38: else
39:    goto End
40: end if
41: End
```

Tor Connection Detection (TorCD)



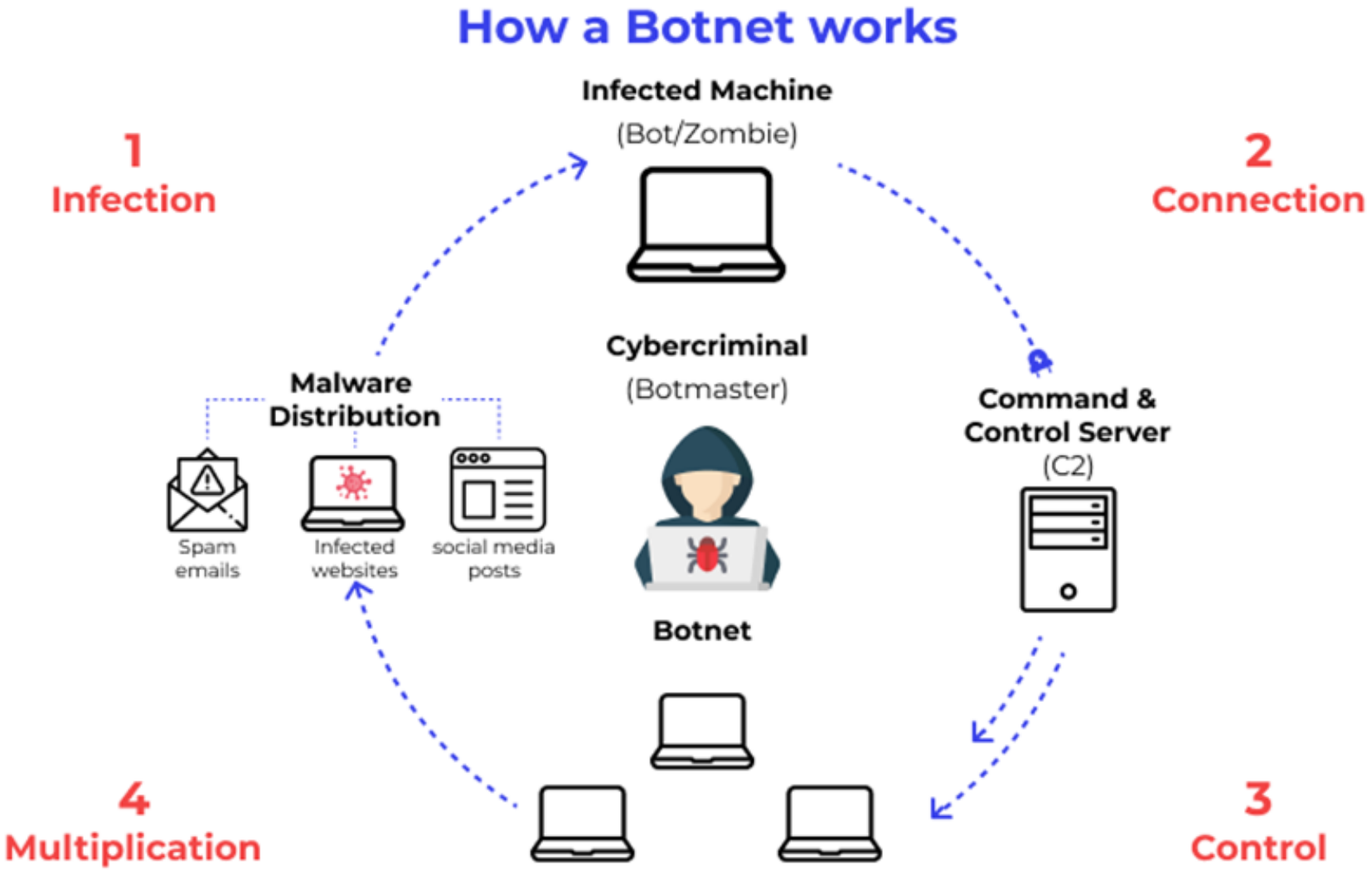
Domain Flux Detection (DFD)

- Domain fluxing is a technique for keeping a malicious attack campaign or botnet in operation by constantly changing the domain name of the Command and Control (C&C) server

Botnet

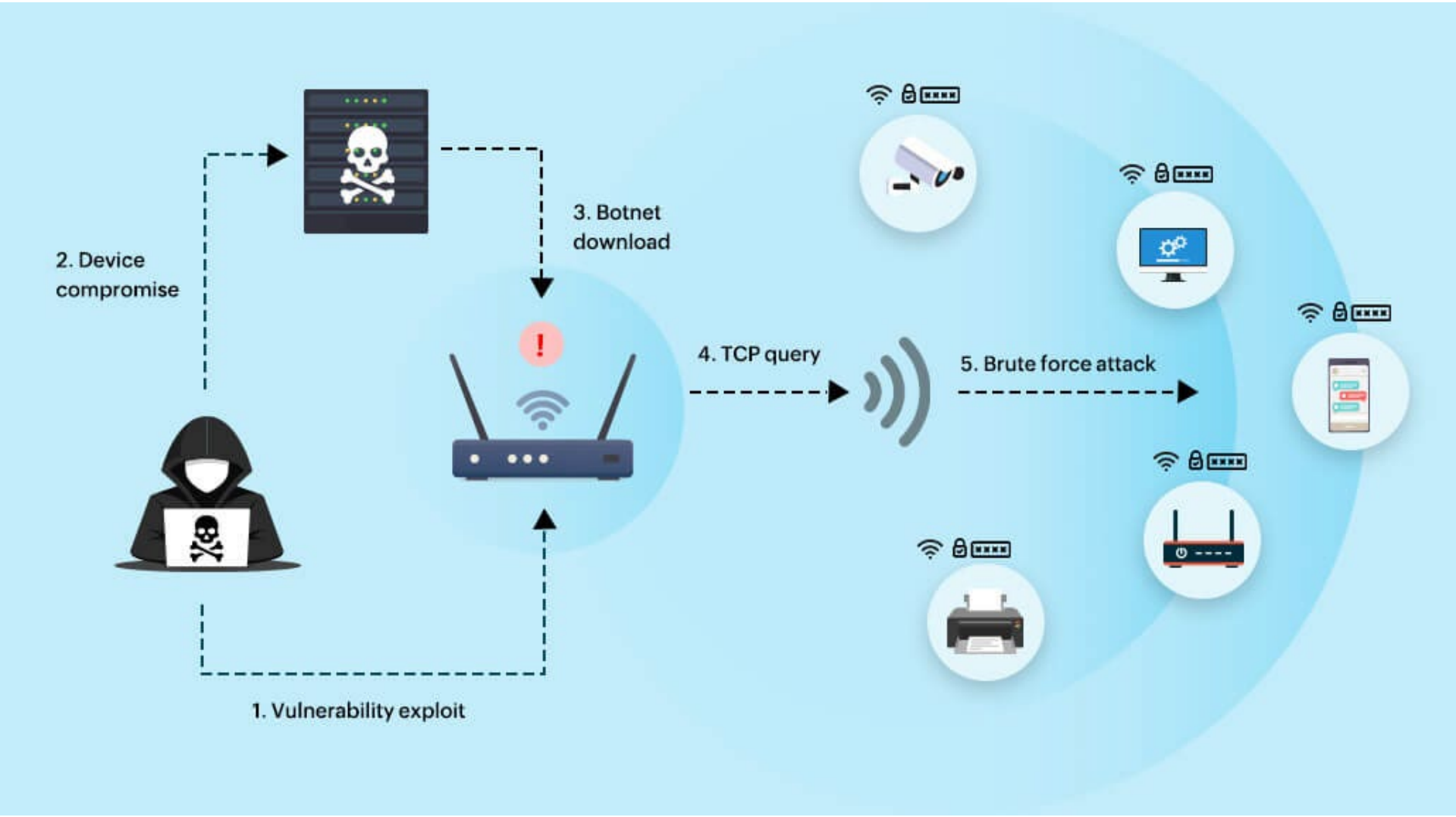
- Botnet is a number of internet-connected devices, which may include personal computers (PCs), servers, mobile devices and Internet of Things (IoT) devices that are infected and controlled by a common type of malware

- Botnets are commonly used to:
  - Send email spam
  - Engage in click fraud campaigns
  - Generate malicious traffic for DDoS attacks (Mirai IoTs)
  - Mine Bitcoin
  - Keyloggers
  - Rent



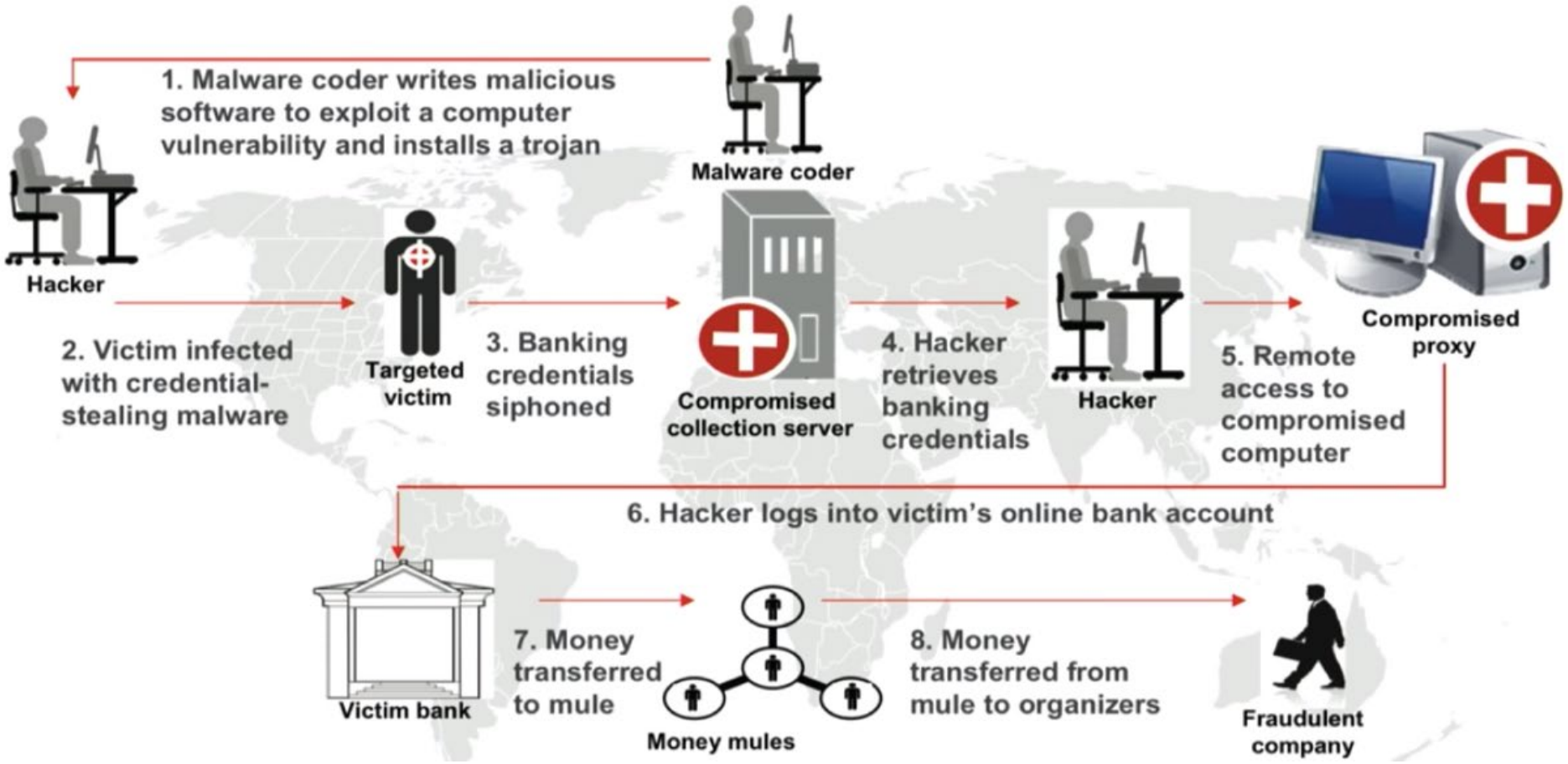
https://www.wallarm.com/what/what-is-a-botnet

Mirai Malware



https://www.manageengine.com/log-management/cyber-security/mirai-botnet-attack.html

Zeus – A Botnet for Stealing Money



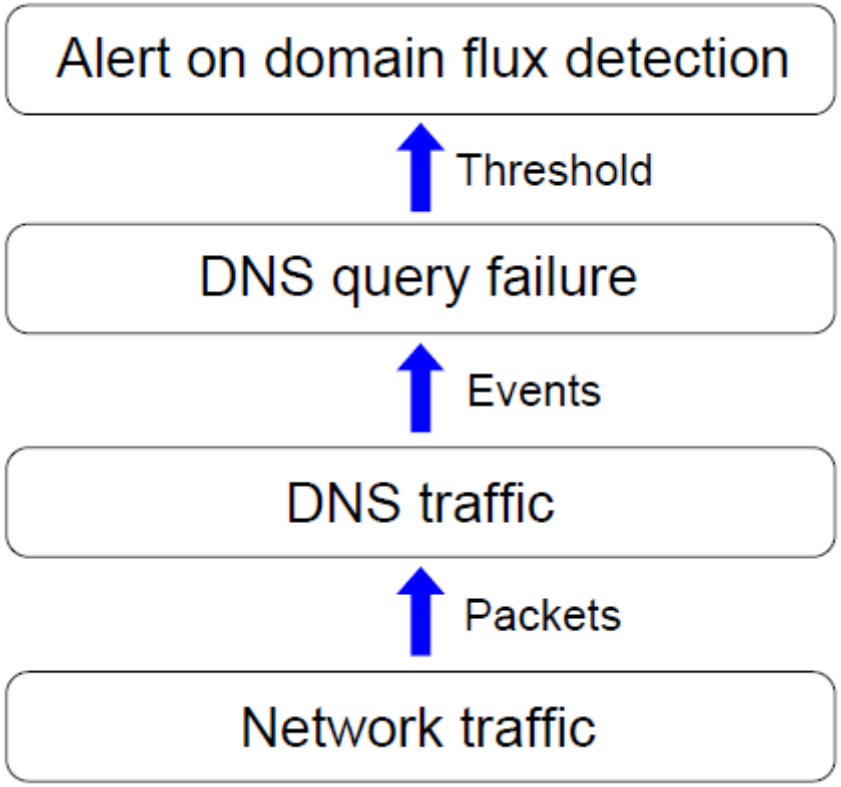
https://en.wikipedia.org/wiki/Zeus_%28malware%29

Domain Flux Detection (DFD)

Algorithm 7 Implementation pseudo-code of DFD

```
1: Get dns_failure_threshold
2: Extract DNS traffic
3: Get dns_message event
4: if the connection is established by a host from the monitored
5:     network then
6:     if dns_message event is due to DNS error of NXDOMAIN then
7:         if the host IP is not in t_dns_failure table then
8:             write host IP into t_dns_failure
9:             host IP counter ← 1
10:        else
11:            Increase host IP counter by 1
12:            if host IP counter > dns_failure_threshold then
13:                Delete host IP from t_dns_failure
14:                Reset host IP counter to zero
15:                if the same domain_flux_alert has been generated
16:                    over the last day then
17:                    goto End
18:                else
19:                    Generate an event (domain_flux_alert)
20:                    Write domain_flux_alert into domain_flux.log
21:                    Send an alert email to RT
22:                    Suppress the same domain_flux_alert over the
23:                    next day
24:                end if
25:            else
26:                goto End
27:            end if
28:        end if
29:    else
30:        goto End
31:    end if
32: else
33:    goto End
34: end if
35: End
```

Domain Flux Detection (DFD)



Acknowledgement

This material uses resources from:

- I. Ghafir, K. G. Kyriakopoulos, S. Lambotharan, F. J. Aparicio-Navarro, B. Assadhan, H. Binsalleeh and Diab M. Diab, “Hidden Markov Models and Alert Correlations for the Prediction of Advanced Persistent Threats,” IEEE Access, 2019.
- I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han and R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, “Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis,” Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.
- Verma, R.M. and Marchette, D.J., 2019. Cybersecurity Analytics. CRC Press.
- Cyber Security Tutorial - Cyber Security Training For Beginners. Simplilearn.
- Humayun, M., Niazi, M., Jhanjhi, N.Z., Alshayeb, M. and Mahmood, S., 2020. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, pp.1-19.
- Madarie, R., 2017. Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. International Journal of Cyber Criminology, 11(1).
- Akbanov, M., Vassilakis, V.G. and Logothetis, M.D., 2019. WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology.