TorBot: Protecting the Tor Network against Malicious Traffic

Advisor: Paulo Lício de Geus

Marcelo Invert Palma Salas (PhD Candidate @UNICAMP)

Esdras Rodrigues Do Carmo (Scientific Initiation Fellow)

Vitor Falcão da Rocha (Scientific Initiation Fellow)

University of Campinas

With support from Frida Lacnic Finance Agency

The Tor Network

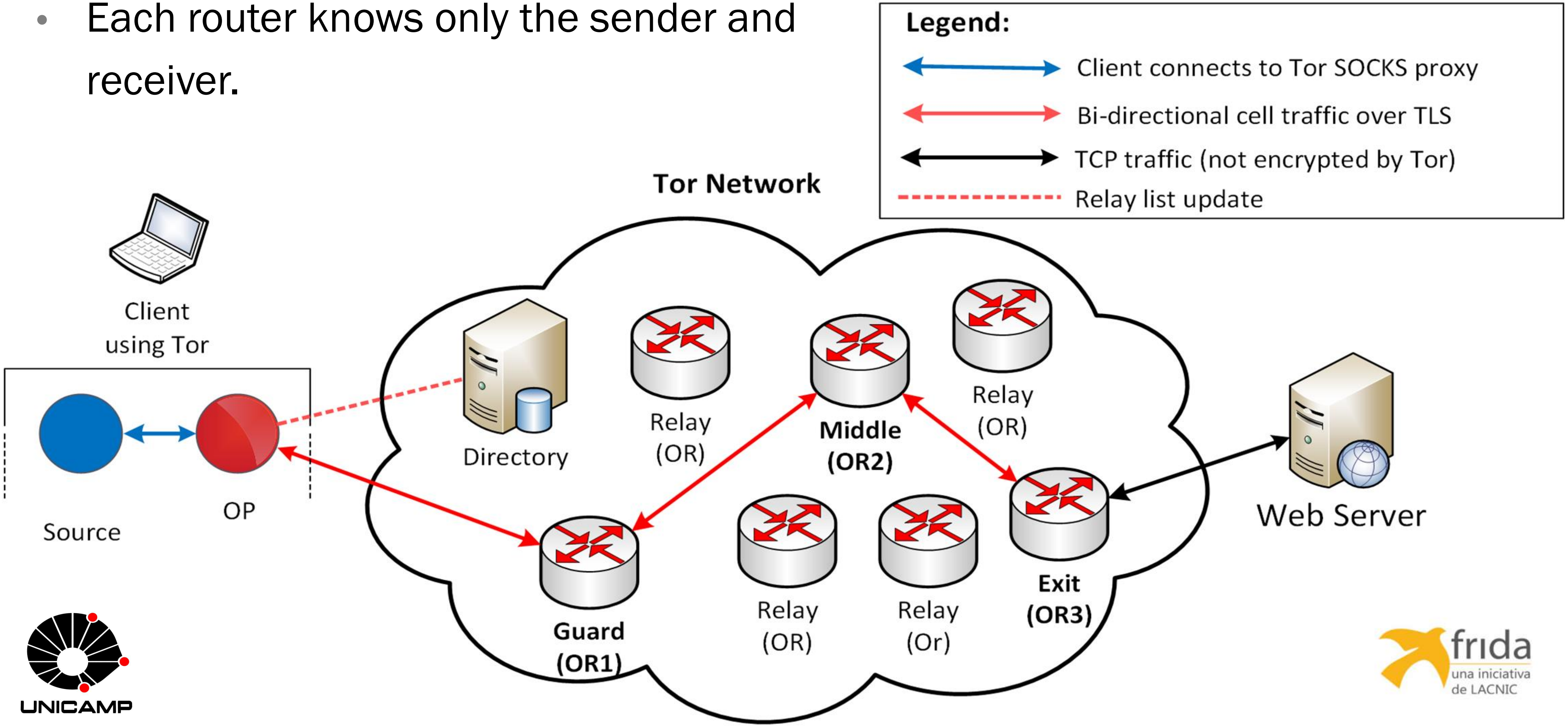
- … is an overlay network that enables anonymous communication between applications that communicate over TCP [1]. protecting your privacy and identity on the Internet.

- Tor also protects our data against corporate or government targeted mass surveillance.

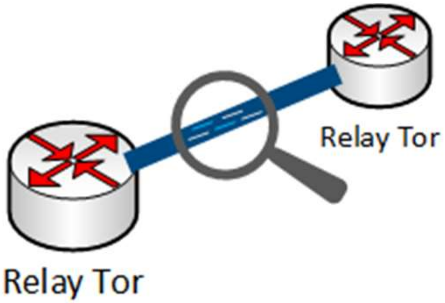
- Despite being used mainly by activists, journalists and bloggers, it supports illicit services and is prone to carry 30X more malicious traffic compared with others networks [2].

How does Tor Work?

- Tor is a group of volunteer–operated servers.
- Composed by 3 relays (guard, middle and exit), it applies distributed security to the network.
- Each router knows only the sender and receiver.

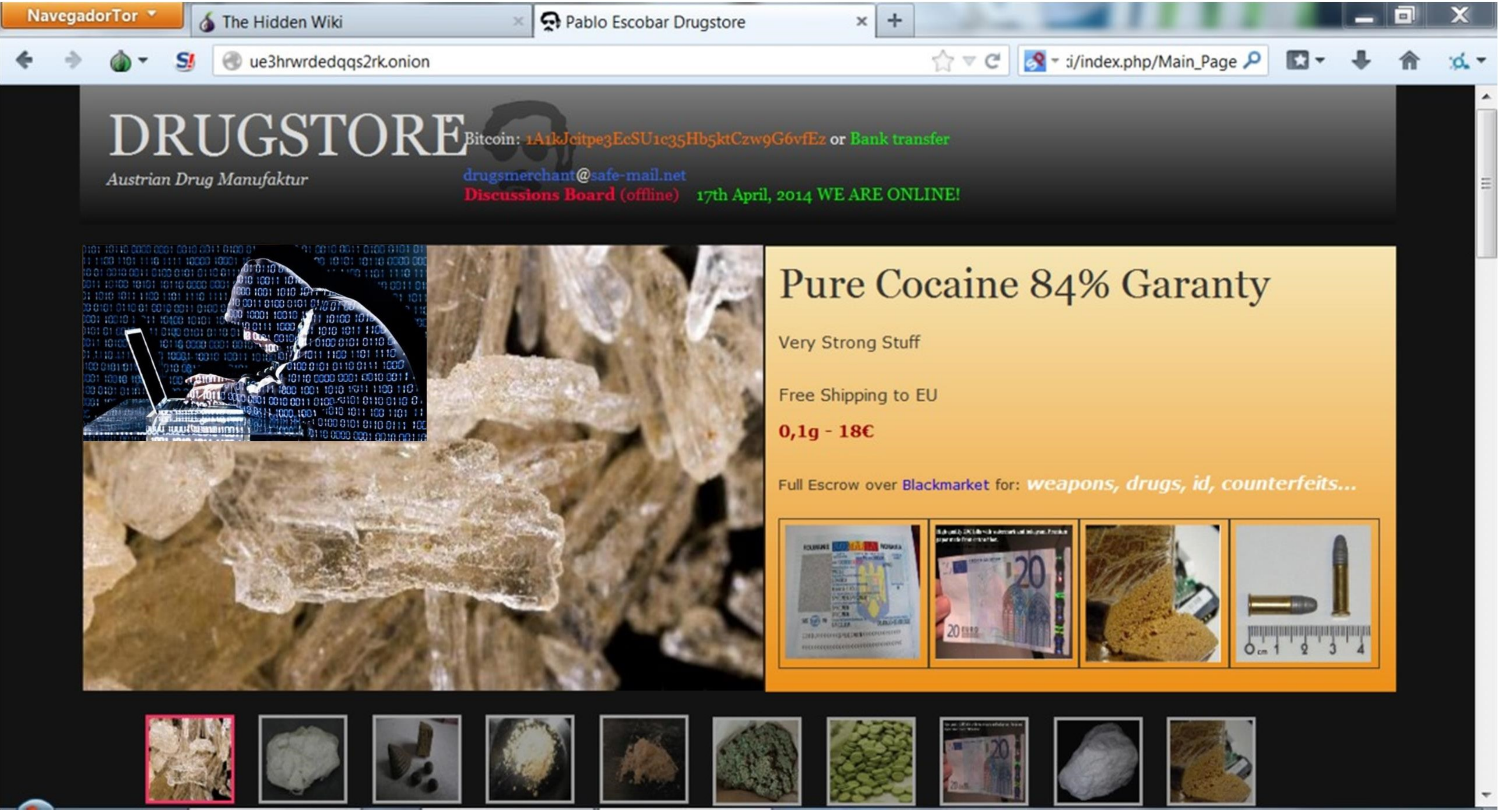


Deep problems in the deep web



- Governmental Vigilance (In particular Exit Relay and spoofing Hidden Services (HS))
- Connection speed (New competition: Rifle - MIT, I2P, Freenet)

- Malicious Traffic:
  - P2P (BitTorrent)
  - Hackers
  - Malware (botnets, rasomware (WannaCry))
  - Illegal Markets (drugs, counterfeit products, cigars, medicines) <=> gray market {Aliexpress, DHgate, iOffer}
  - HS (are 2% of Tor traffic, 1.5% are malicious traffic).
  - Kidnappers and blackmailers (rescue -> Bitcoins, Ripple, Ethereum, NEM, Litecoin, & among others)



DRUGSTORE

Austrian Drug Manufaktur

Bitcoin: 1A1kJcitpe3EcSU1c35Hb5ktCzw9G6vfEz or Bank transfer

drugsmerchant@safe-mail.net

Discussions Board (offline) 17th April, 2014 WE ARE ONLINE!

Pure Cocaine 84% Garanty

Very Strong Stuff

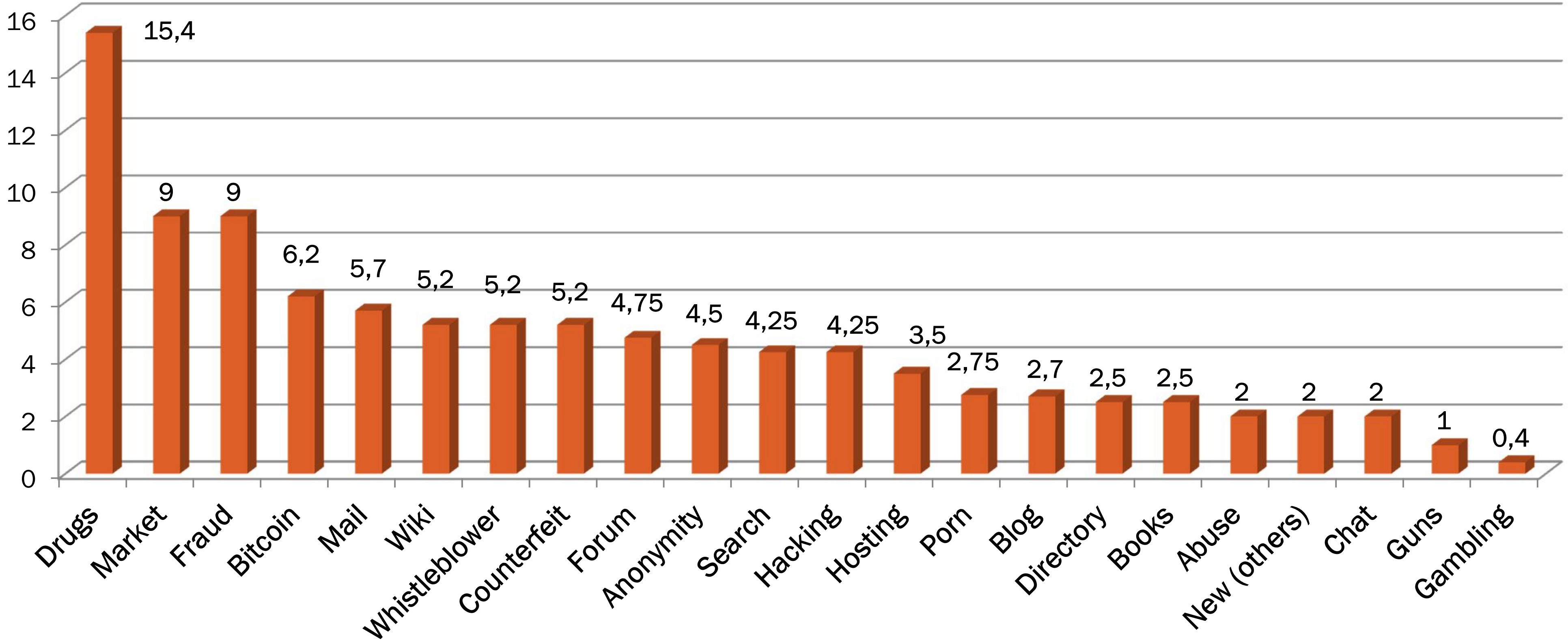
Free Shipping to EU

0,1g - 18€

Full Escrow over Blackmarket for: ***weapons, drugs, id, counterfeits...***

State of the Art of the Hidden Services in Tor

- In [3], the authors analyzed more than 80.000 hidden services, finding:
  - 85% of HS are up for less than 5 days,
  - +100 new HS come online,
- There is increased usage by malware (botnets, ransomware, etc.) in relation to the surface web.



How Malicious Traffic Works in Tor?

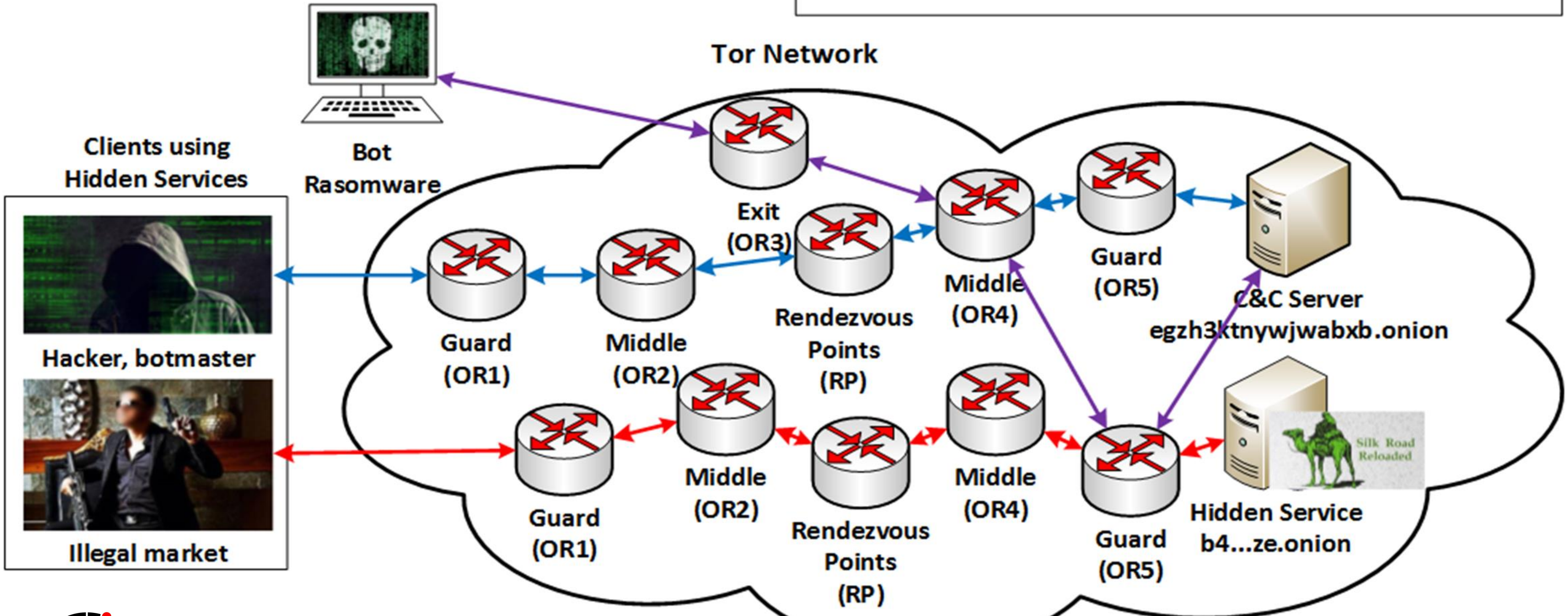
- Malware (botnets, rasomware, ...)
- Illegal market (drugs, guns, ...)
- Bitcoin (anonymous transactions)

Legend:

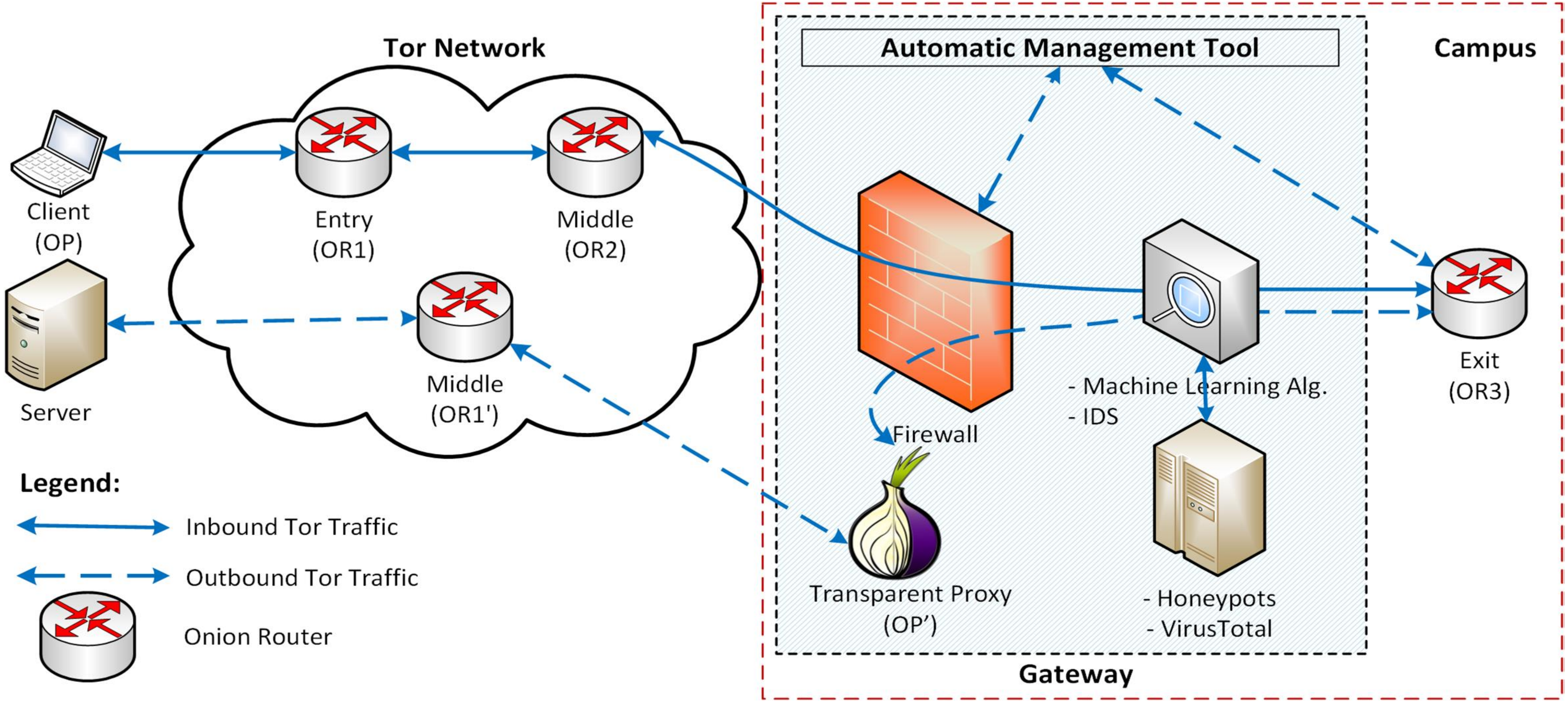
↔ Botmaster connects to C&C over Tor (Zeus)

↔ Client connects to the Silk Road Reload

↔ C&C collects and sends data to zombie computer



Architecture for Discovering and Blocking Malicious Traffic



Protecting the Tor Network against Malicious Traffic

- Our proposal is divided into three phases:

  i) Collect; ii) analysis and classification; iii) tracing and blocking malicious traffic.

- This include:

  Setting up a network capture and re-routing of the benign traffic;

  System development for analyzing, back tracing, and blocking malicious traffic like botnets and others malware;

  An application to recognize and block malicious hidden services.

- To achieve this goal, we propose using tools such as:

  Traffic analyzers;

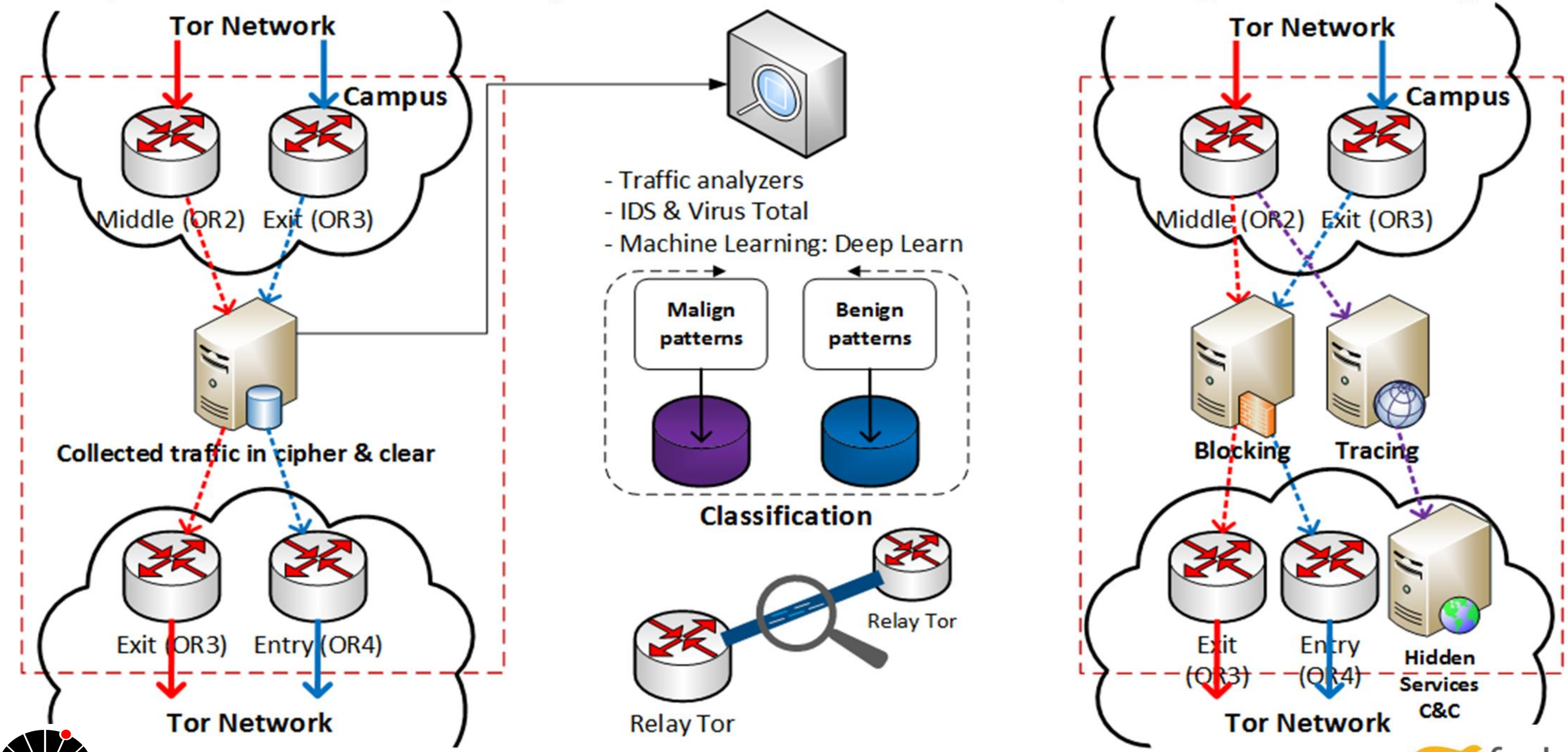
  IDS and VirusTotal;

  Machine learning techniques and metadata analyzing.

Protecting the Tor Network against Malicious Traffic

- Our proposal is divided into three phases:

i) Collect ii) Analysis and Classification iii) Tracing and Blocking



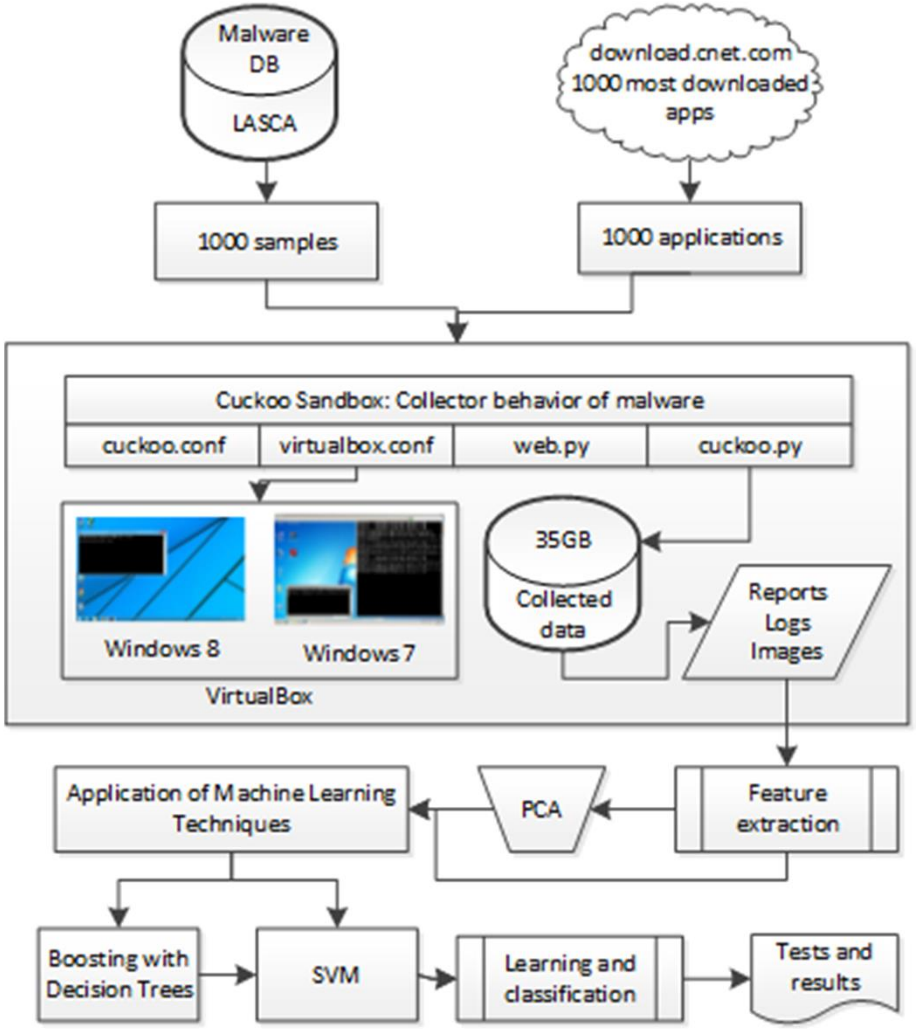
------------------------malicious traffic------------------------

Collect Malicious Traffic

More than 1200 samples:

- http://cerberussssc7cat.onion/
- https://zeltser.com/malware-sample-sources/
- https://github.com/ytisf/theZoo
- https://github.com/aboutsecurity/malware-samples
- https://github.com/ashishb/android-malware
- https://github.com/fdiskyou/malware
- https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168 (WannaCry)

Analysis and Classification Malicious Traffic

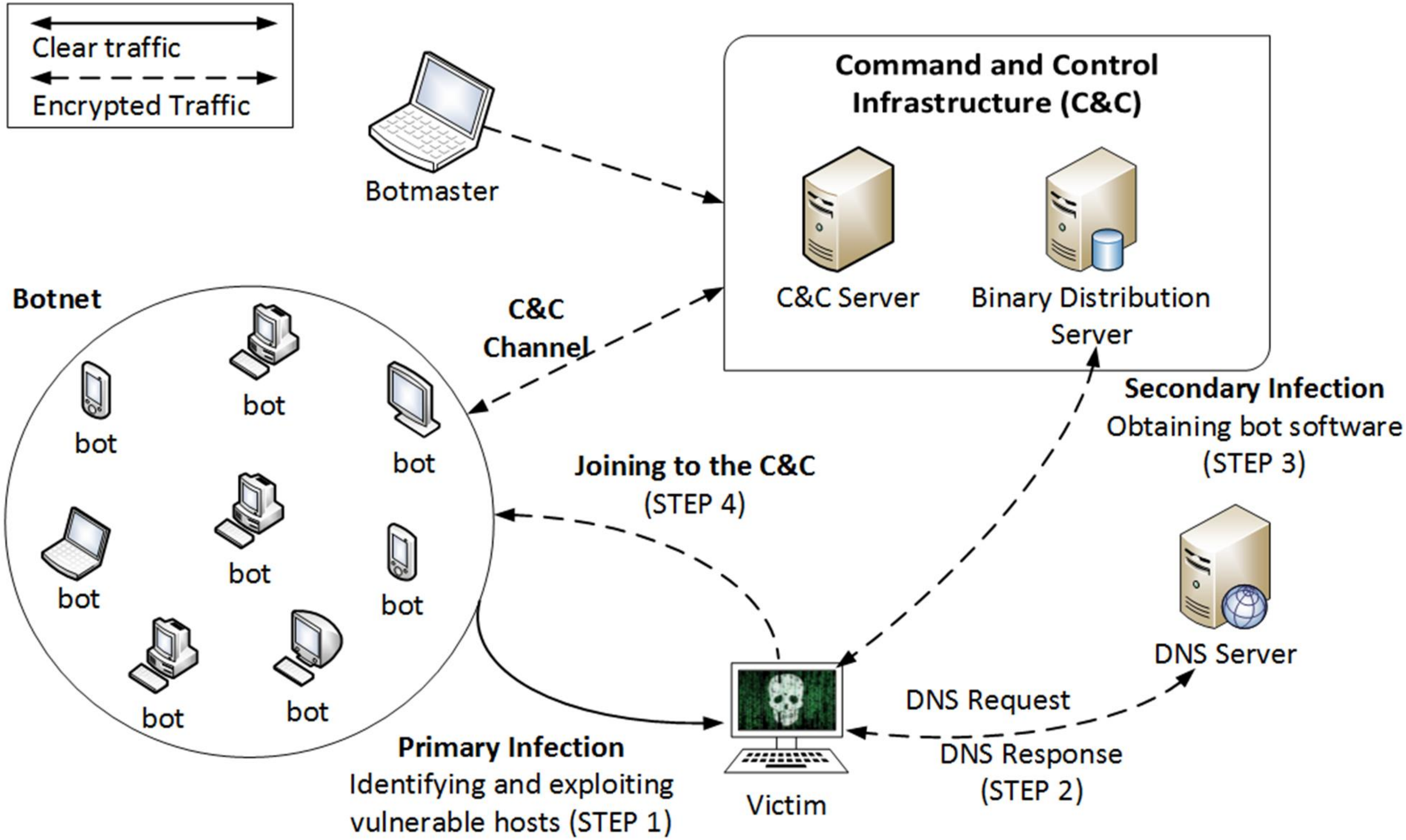


Some Results for Windows 8.1:

- *Decision Tree: 96.15%*
- *Gaussian Naive Bayes: 96.44%*
- *Multinomial Naive Bayes: 94.49%*
- *Neural Network MLP: 97,7%*
- *SVM: 98,22%*

- *WannaCry was detected by 4/5 algoritms.*

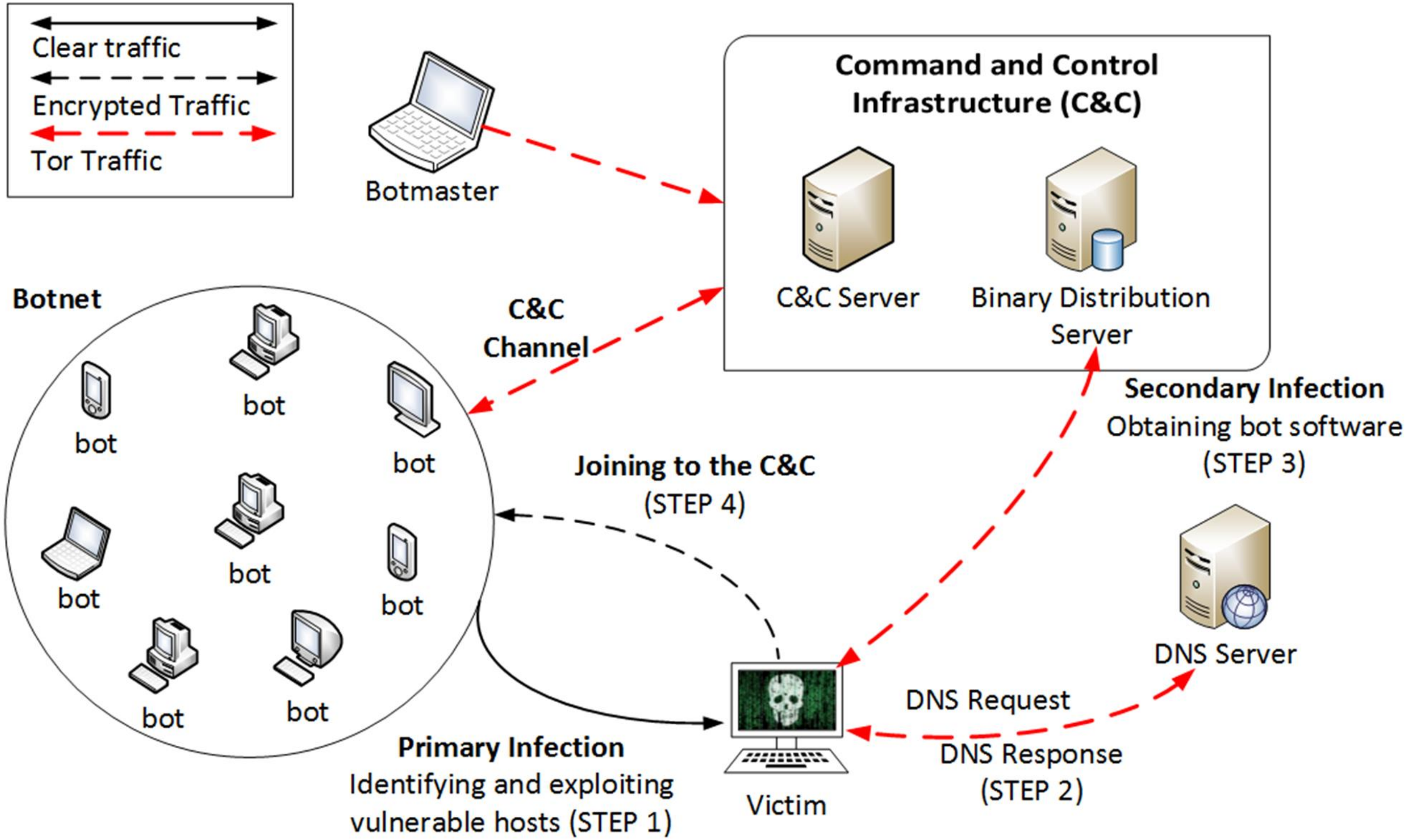
How does a botnet work?



UNICAMP

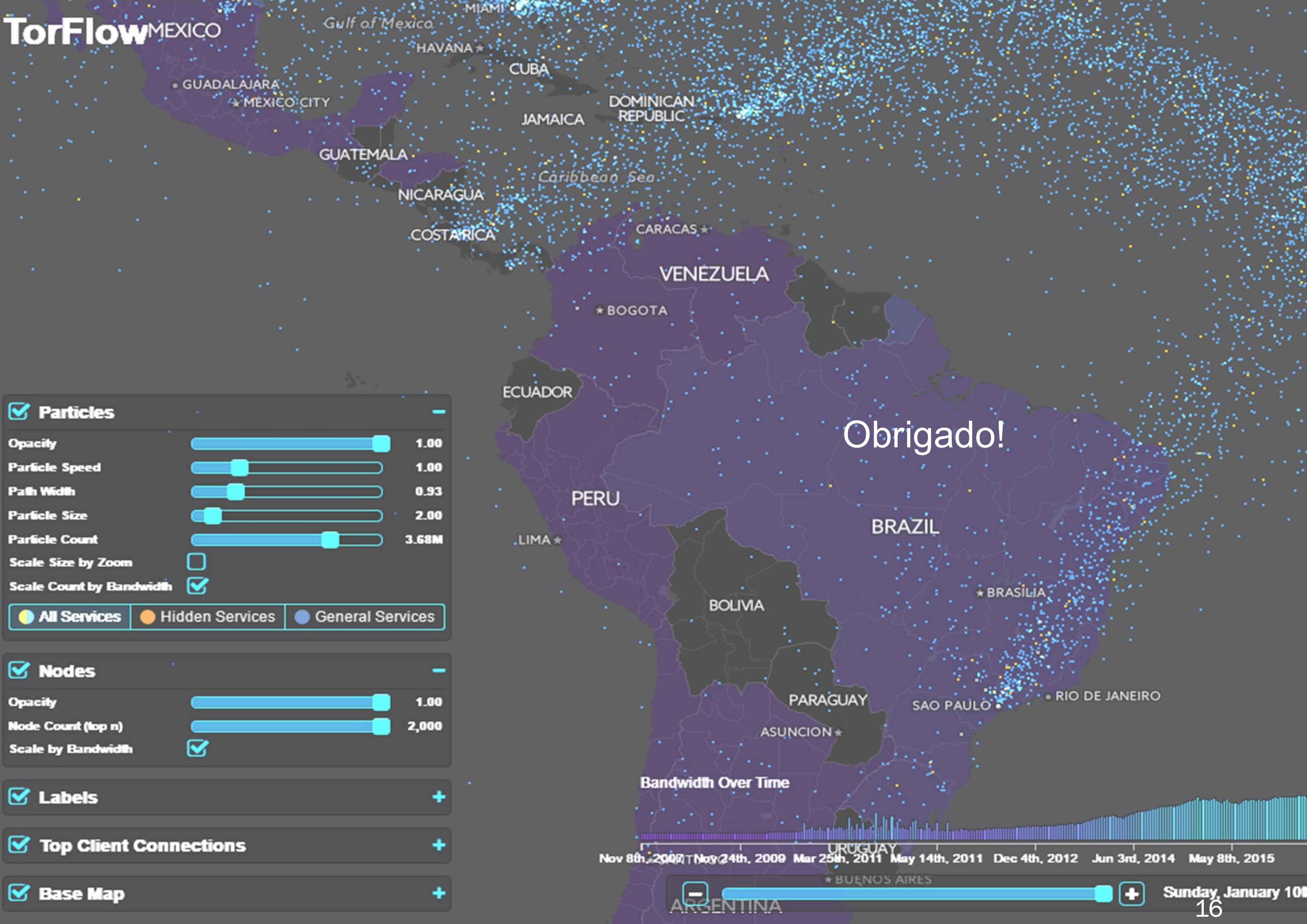
frida una iniciativa de LACNIC

How does a botnet work with Tor?



References

1. Zhen Ling, Junzhou Luo, Kui Wu, Wei Yu, and Xinwen Fu. Torward: Discovery, blocking, and traceback of malicious traffic over tor. Information Forensics and Security, IEEE Transactions on, 10(12):2515-2530, Dec 2015.
2. Tor metrics. https://metrics.torproject.org/, 2015.
3. Owen, Gareth, and Nick Savage. "Empirical analysis of Tor Hidden Services."*IET Information Security* (2015).
4. Gandeva B. Satrya, Niken D.W. Cahyani, and Ritchie F. Andreta. The detection of 8 type malware botnet using hybrid malware analysis in executable file windows operating systems. In Proceedings of the 17th International Conference on Electronic Commerce 2015, ICEC '15, pages 5:1 5:4, New York, NY, USA, 2015. ACM.
5. A. Sanatinia and G. Noubir. Onionbots: Subverting privacy infrastructure for cyber attacks. pages 69-80, June 2015.



Obrigado!

☑ Particles −

Opacity 1.00

Particle Speed 1.00

Path Width 0.93

Particle Size 2.00

Particle Count 3.68M

Scale Size by Zoom □

Scale Count by Bandwidth ☑

All Services | Hidden Services | General Services

☑ Nodes −

Opacity 1.00

Node Count (top n) 2,000

Scale by Bandwidth ☑

☑ Labels +

☑ Top Client Connections +

☑ Base Map +

Bandwidth Over Time

Nov 8th, 2007 Nov 24th, 2009 Mar 25th, 2011 May 14th, 2011 Dec 4th, 2012 Jun 3rd, 2014 May 8th, 2015

Sunday, January 10th