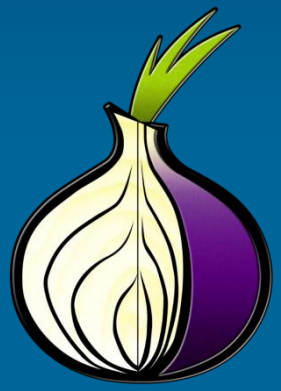
TorBot - Protecting the Tor Network against Malicious Traffic

EnSI - VII Encontro de Segurança em Informática do CERT.Bahia



Orientador: Paulo Lício de Geus

Marcelo Invert Palma Salas (Doutorando)

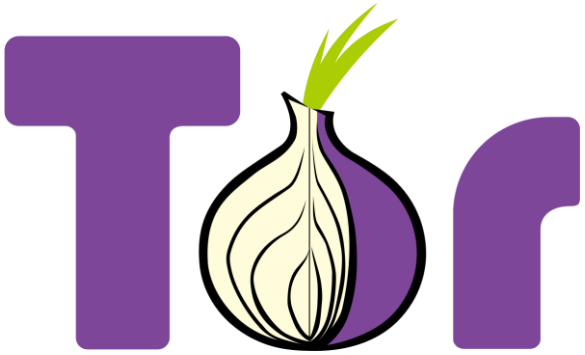
André Almeida, Esdras Rodrigues e Marcus Danilo

(Iniciação Científica)

Universidade Estadual de Campinas

Com apoio de Frida - LACNIC

O que é a rede Tor?



- Tor é uma rede de camadas operadas por voluntários que funciona com protocolos TCP, provendo ao usuário anonimato e privacidade na internet [1].

- Com +7000 servidores (*onion router* ou *relays)*, é propensa a transportar 30X mais o tráfego malicioso em comparação a outras redes [2].

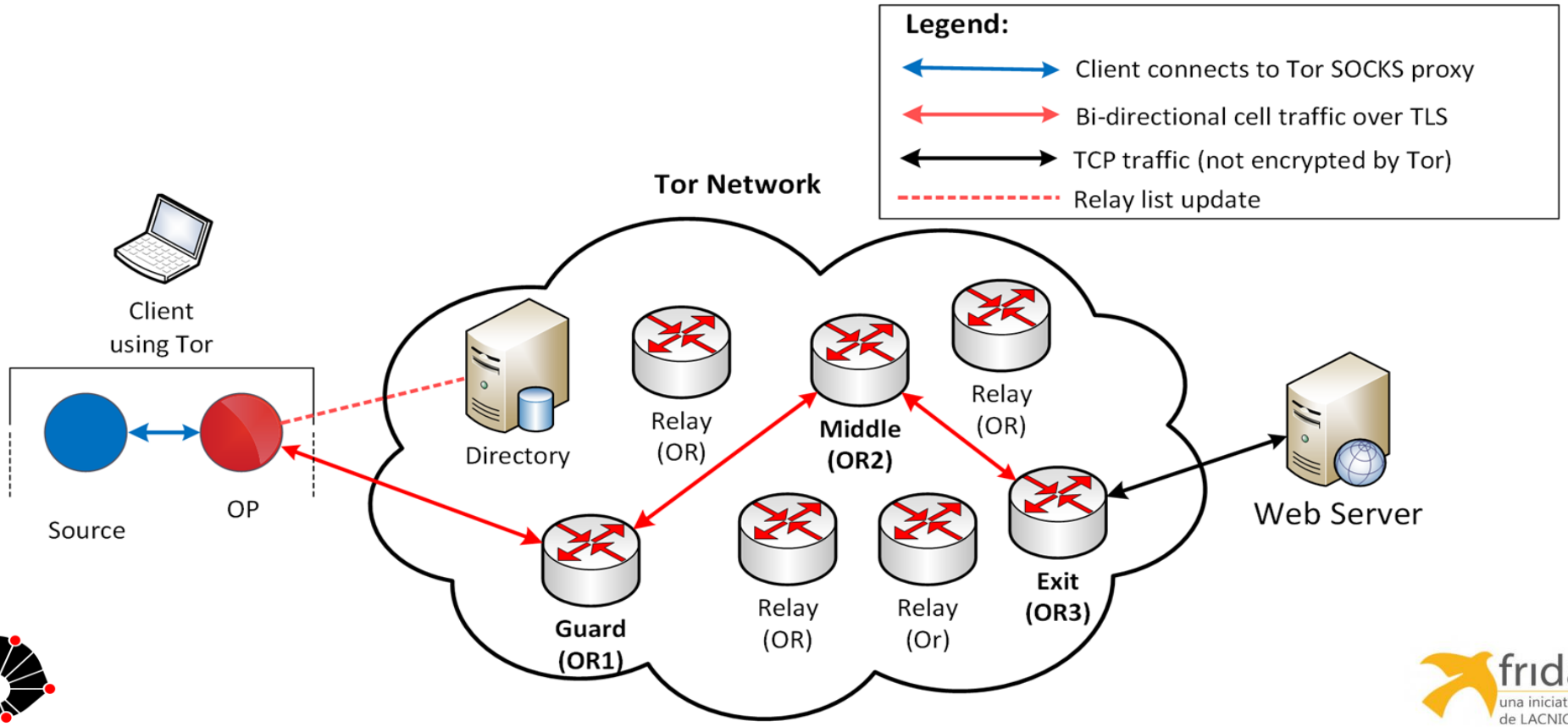
- Criada com a finalidade de proteger dados de navegação contra espionagem governamental e coleta abusiva de dados por empresas. Tor está em constante crescimento.

UNICAMP

frida
una iniciativa
de LACNIC

Como funciona a rede Tor?

- A rede Tor consiste em um conjunto de voluntários que executam *relays* (nós).
- Cada vez que um cliente se conectar a um serviço a través de Tor, ele cria um circuito composto por 3 *relays* (*guard*, *middle* e *exit*).
- Cada *relay* conhece apenas os seus vizinhos.



Serviços Ocultos sobre Tor

- Tor permitem aos serviços da internet e os clientes ocultar suas comunicações através de serviços ocultos (*hidden service*).
- Não fornecem suas IPs
- Usam Pontos de Encontro ou (*Rendezvous Points* - RP).
- O proxy do cliente e o serviço da Internet enviam suas mensagens a um RP.
- O estabelecimento de um serviço oculto utiliza o encaminamento cebola.

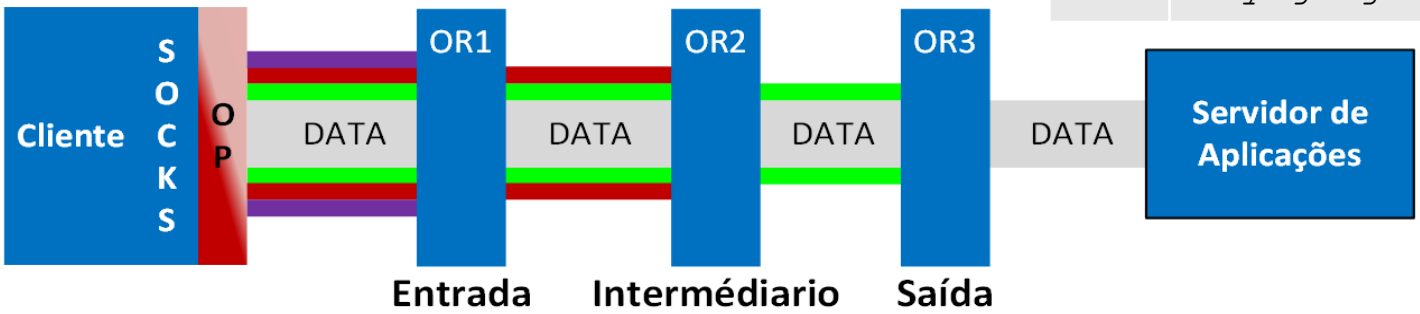
Mau emprego dos SO

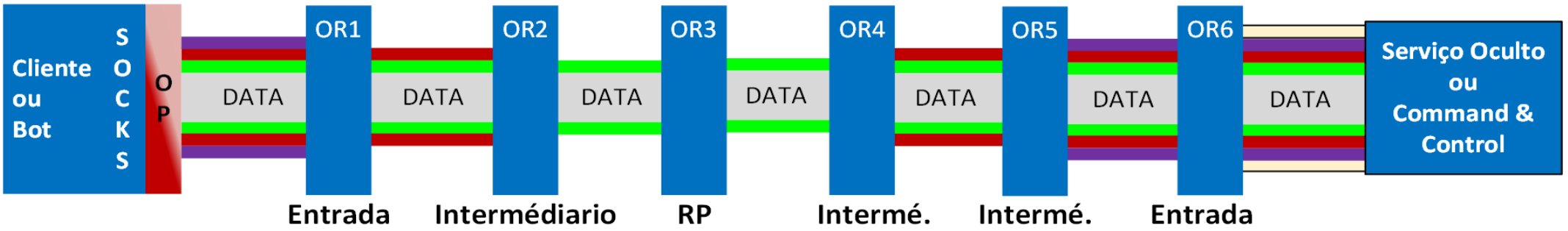
O mau emprego dos SO pemitiu a criaçào da Dark Web → Silk Road ($us. 1,9M) e outras serviços.

O tráfego de Bot ↔ C&C ↔ botmaster representam o 10% do tráfego malicioso segundo [2].

Um dos mais conhecidos: Skynet

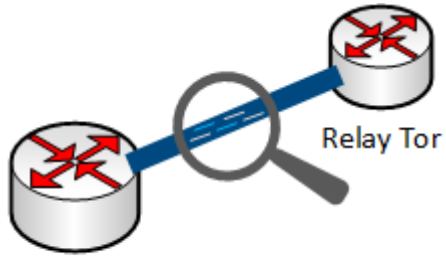
	Onion	Description
1	177ukkijtdca2tsy	Sefnit
2	pomyeadfnmtn544p	Sefnit
3	qxc7mc24mj7m4e2o	Sefnit
4	7sc6xyn3rrxtknu6	Sefnit
5	lorpzyxqxscsmscx	Sefnit
6	7fyipi6vxyhpcouy	Sefnit
7	xlrb3h5gyswyxdc5	Kaziarb
8	6tlpoektcb3gudt3	Sefnit
9	xvauhzlpkirnzghg	Skynet
10	f2ylgv2jochpzm4c	Skynet





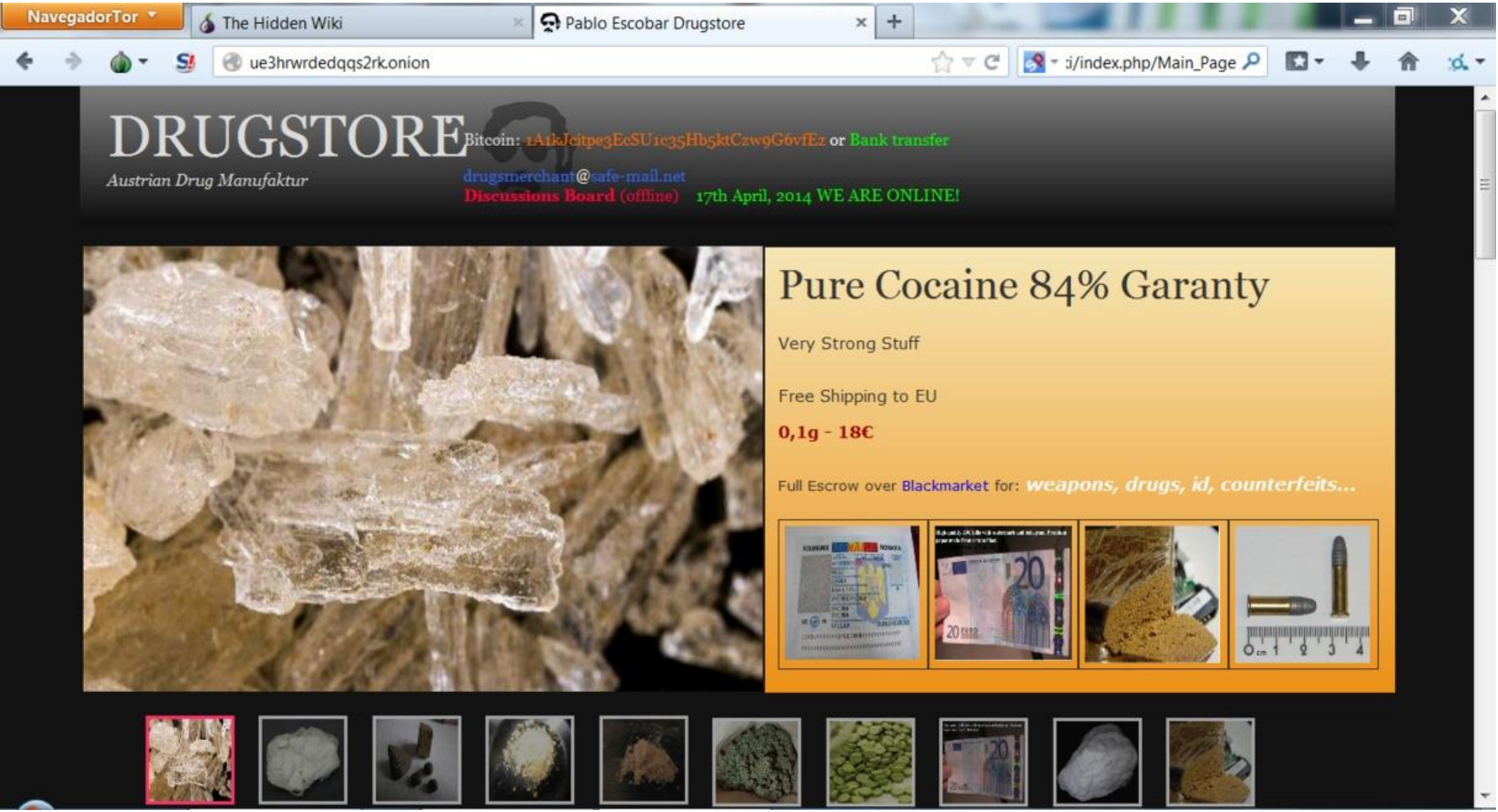
Problemas na rede Tor

- Vigilância governamental, principalmente nos *relays* de saída.
- Alta latência na rede, devido ao redirecionamento constante de tráfego.
- Tráfego malicioso:
- Pirataria transferida por BitTorrent;
- Hackers;
- Propagação e comunicação de malwares (Ransomware, Botnet
- Hospedagem de mercados ilegais (drogas, armas, etc.) e conteúdos ilícitos (pornografia infantil, etc.);
- Sequestro de dados e chantagens (com pagamentos em criptomoedas).



UNICAMP

frida
una iniciativa de LACNIC

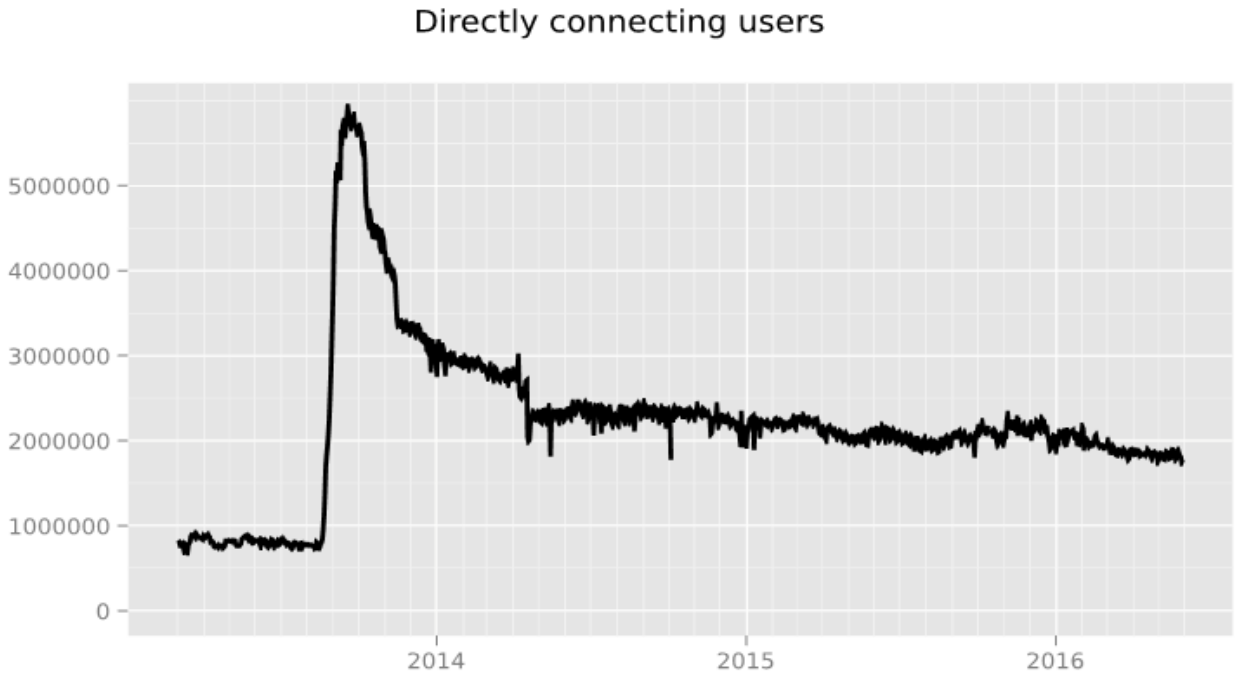


UNICAMP

frida
una iniciativa
de LACNIC

Efeito do Tráfego Malicioso na Rede Tor

- A botnet Mevade/Sefnit começou a transmitir informação a partir de milhões de computadores infectados (bots) para a C&C e vice-versa.
- Gerou um incremento da carga de processamento nos roteadores Tor causado pela grande construção de circuitos Tor.
- O tempo médio de download de um arquivo de 50KB passou de 1,5 a 3 seg.



Projeto TorBot

- Desenvolver técnicas para identificar, classificar e bloquear o tráfego malicioso na rede Tor, protegendo a privacidade dos usuários.

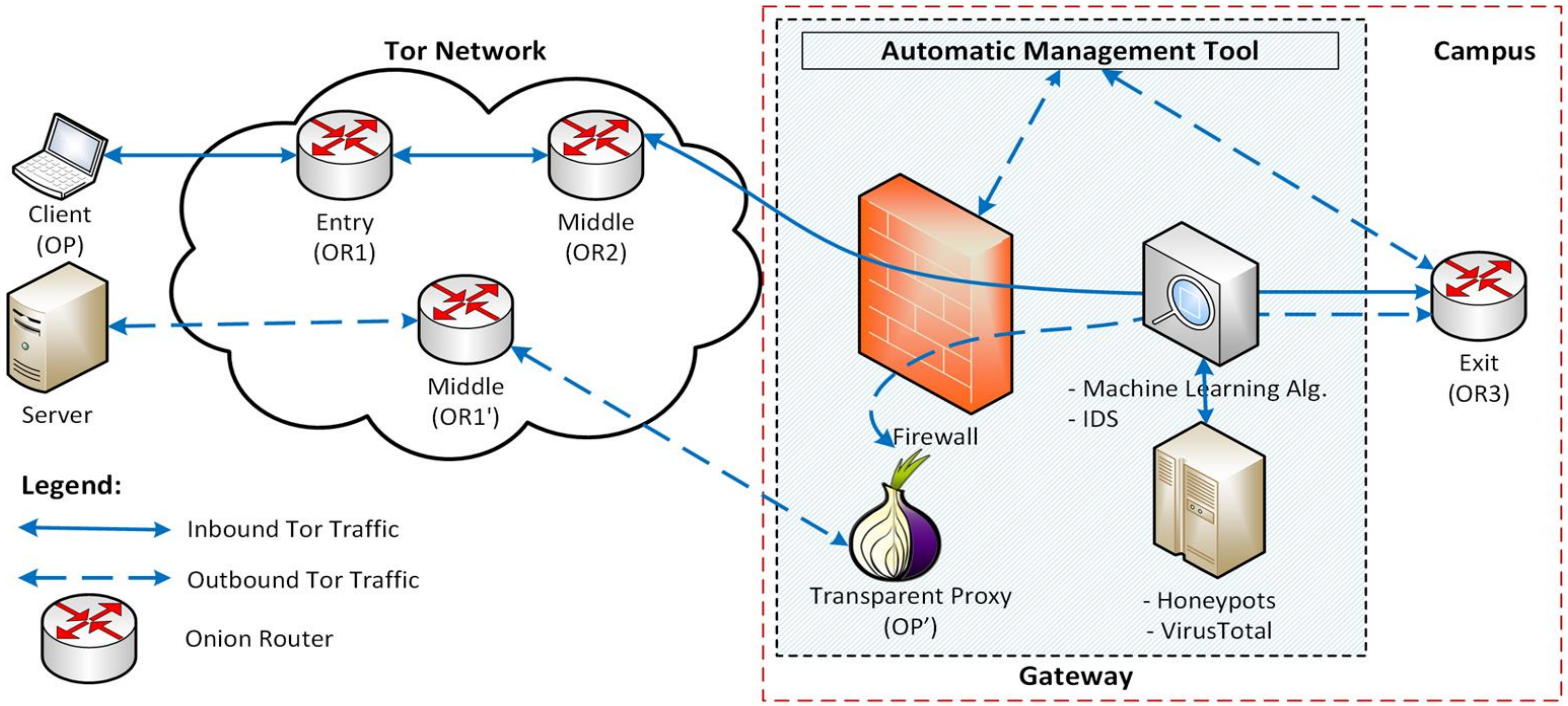
- Sub-projetos:
  - TorSandBox:
    - Coleta, análise e classificação do tráfego (malicioso/benigno) na rede Tor;
  - Tor Crawler:
    - Crawler para análise e classificação de Web Sites .onion na DeepWeb;
  - OnionBots:
    - Detecção, análise e bloqueio de botnets em Tor;

UNICAMP

frida una iniciativa de LACNIC

TorSandBox

- Coleta, análise e classificação do tráfego malicioso na rede Tor através de um nó de saída.
- Utilização de IDS Suricata, Sandbox Cuckoo e VirusTotal.
- Mais de 1500 amostras de binários analisadas em 3 meses.



TorCrawler

- Crawler que percorre a *dark web* (*Hidden Services*) em busca de .onions [4];
- Exemplo de início: http://wiki5kauuihowqi5.onion (Repositório de *HS*s)
- Gera estatísticas (online/offiline) em http://143.106.60.70/
- Alimenta um banco de dados de endereços .onion;

Hidden Services Found

Online	3797
Offline	44216
Total	48035

WebServer

Apache	1889
Nginx	2771
Lighttpd	196
TwistedWeb	41
IIS	43

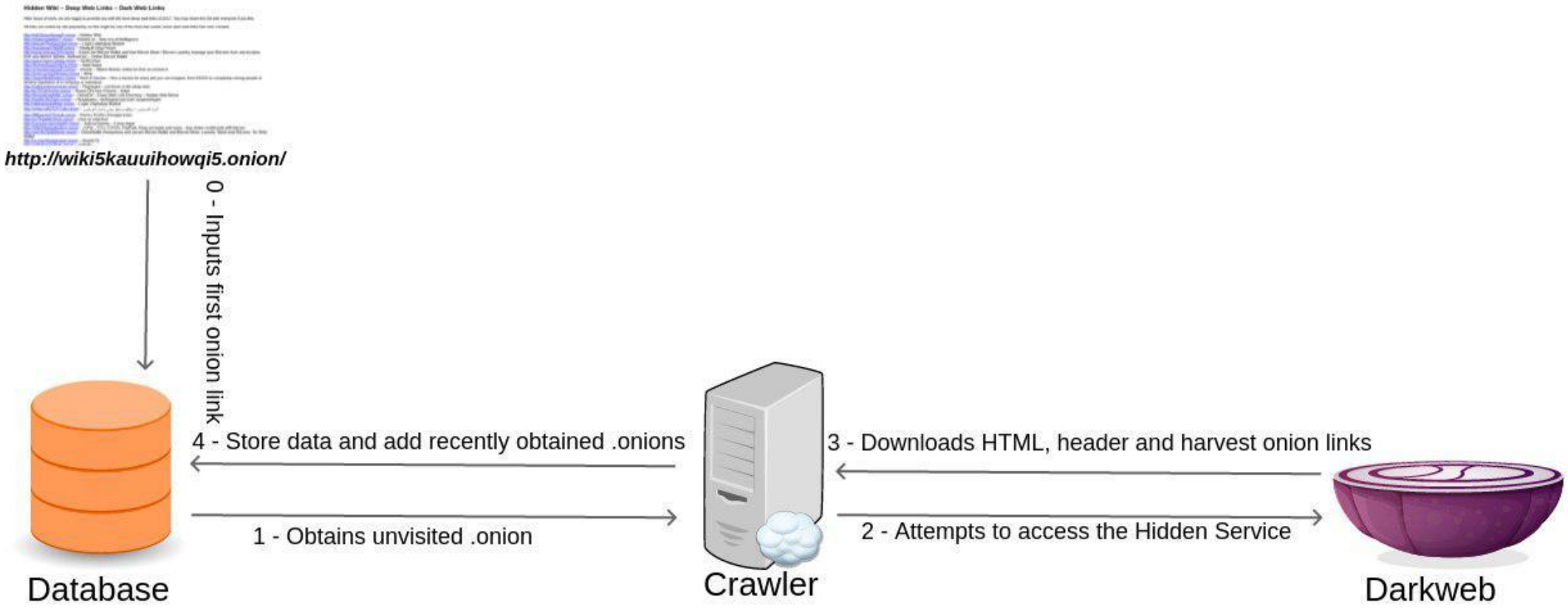
Operating System

Debian	282
Ubuntu	416
CentOs	81
FreeBSD	11
Fedora	6
Suse	1
Windows	98

UNICAMP

frida una iniciativa de LACNIC

TorCrawler


http://wiki5kauuihowqi5.onion/
0 - Inputs first onion link
4 - Store data and add recently obtained .onions
1 - Obtains unvisited .onion
3 - Downloads HTML, header and harvest onion links
2 - Attempts to access the Hidden Service
Database
Crawler
Darkweb

OnionBots

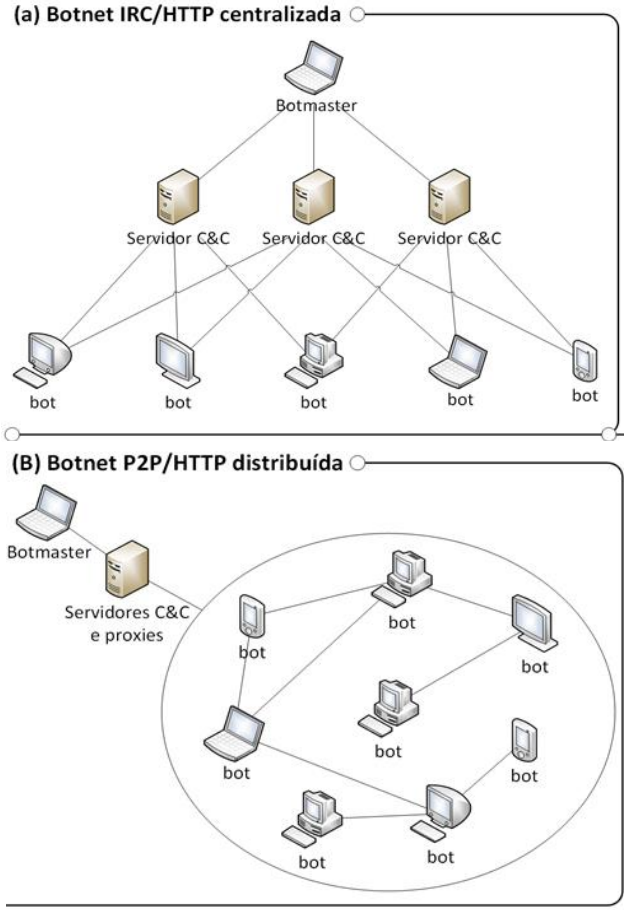
- Computadores infectados (*bots*) que formam uma rede que se comunica via internet (*botnet*). Os recursos computacionais dessas máquinas ficam em disposição ao *Bot Master*.
- Usos mais comuns:
  - Propagação de spam;
  - Mineração de criptomoedas (Bitcoin);
  - Roubo da dados com keyloggers;
  - DDoS;
  - Processamento de dados biomédicos: (https://www.gpugrid.net/about.php).

UNICAMP

frida una iniciativa de LACNIC

OnionBots – Como fazer uma botnet?

- Servidor de controle (*Command & Control or C&C*):
- Centralizados:
  - Menos complexos de se manter;
  - Comunicação mais rápida e direta;
  - Se o servidor cai, a botnet também;
  - Técnicas de fluxo de domínio para mudança dinâmica de servidores (e.g. Torpig, Sta. Barbara Univ. [7]).
- Descentralizado:
  - Vários servidores (ou mesmo outros bots) são usados para passar comandos entre si (e.g. P2P);
  - Se um desses servidores cair, uma parte da rede continua funcionando;
  - Mais complexo de criar;

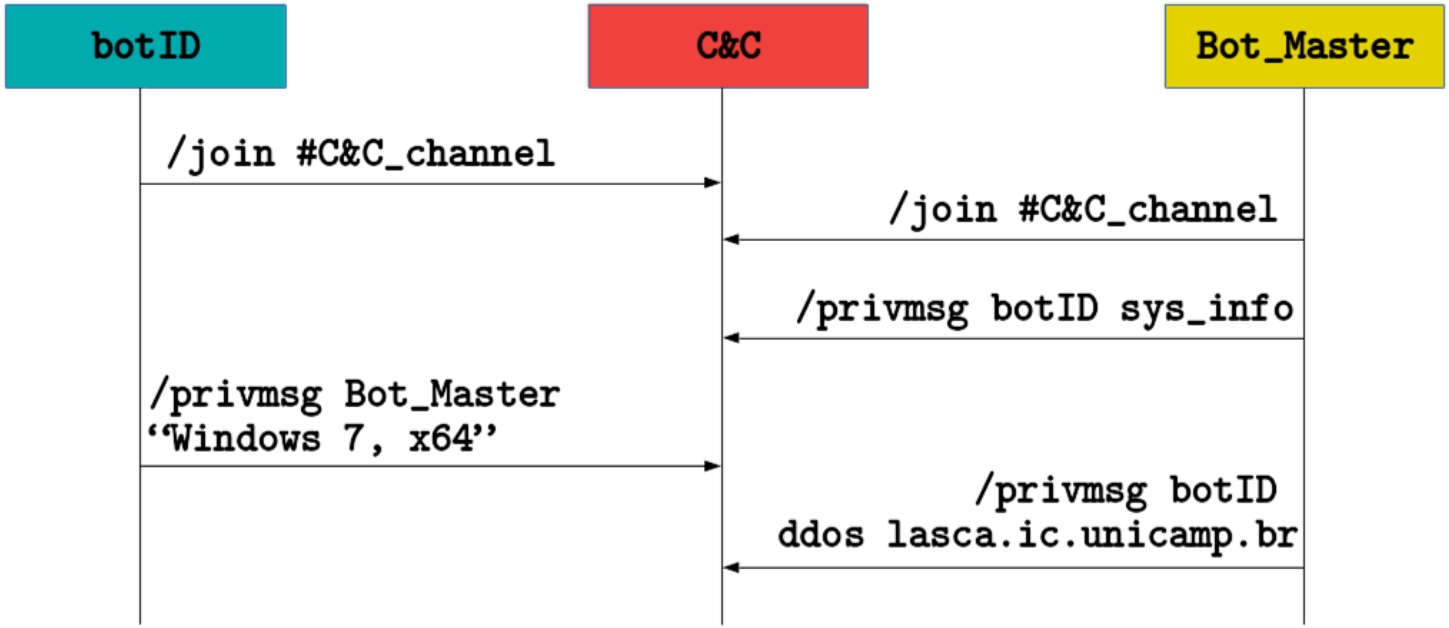


UNICAMP

frida
una iniciativa
de LACNIC

OnionBots – Como fazer uma botnet?

- Protocolos de comunicação: IRC, HTTP, P2P;
- Comunicação criptografada (simétrica/assimétrica);
- IRC (*Internet Relay Chat*):
  - Protocolo criado para troca instantânea de mensagens, privadas ou em grupos;

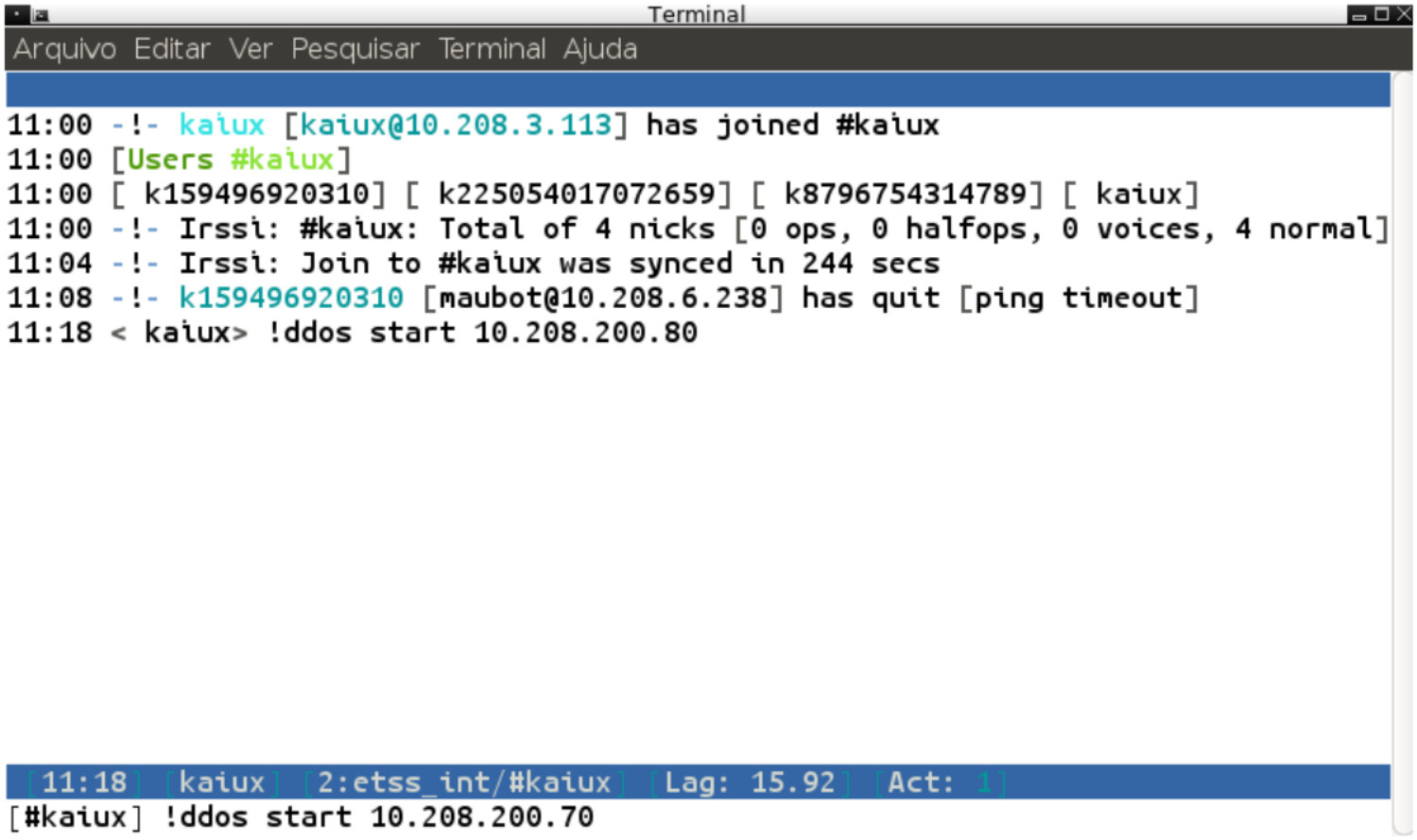


UNICAMP

frida
una iniciativa de LACNIC

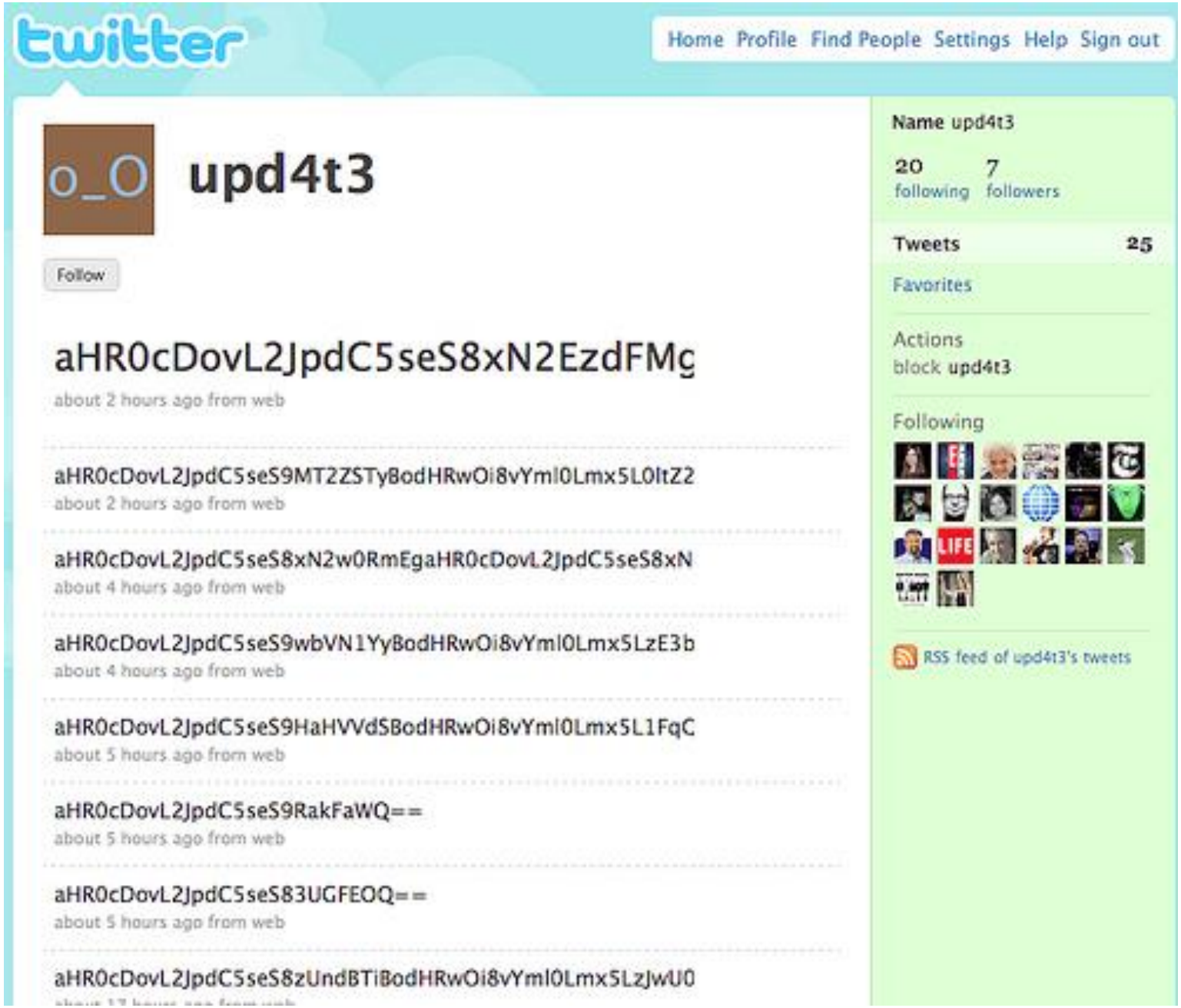
OnionBots – Como fazer uma botnet?

- Fácil escrever um bot que usa um chat;
- Difícil parecer uma conversa realista entre humanos;



UNICAMP

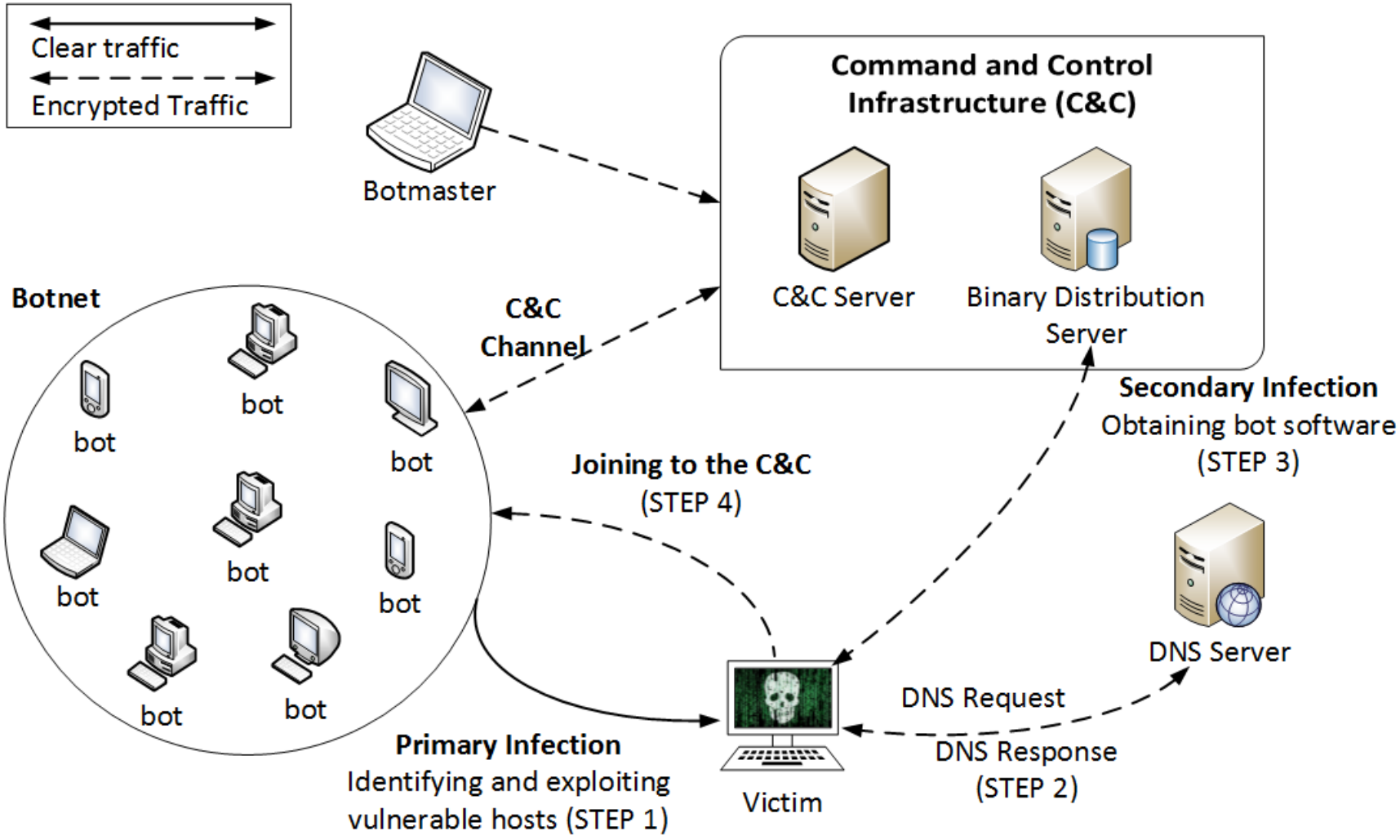
frida una iniciativa de LACNIC



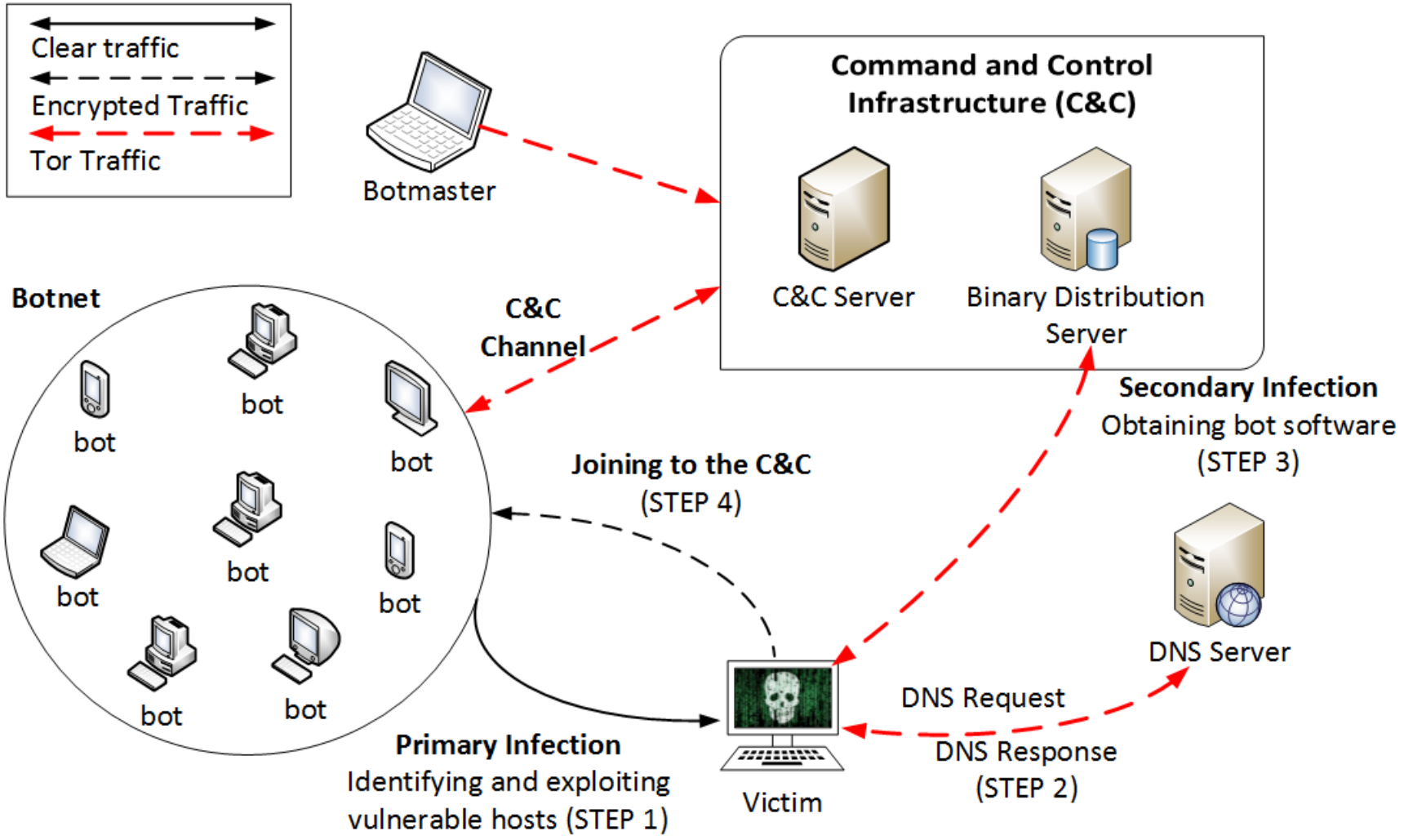
UNICAMP

frida
una iniciativa
de LACNIC

Como funciona uma botnet?



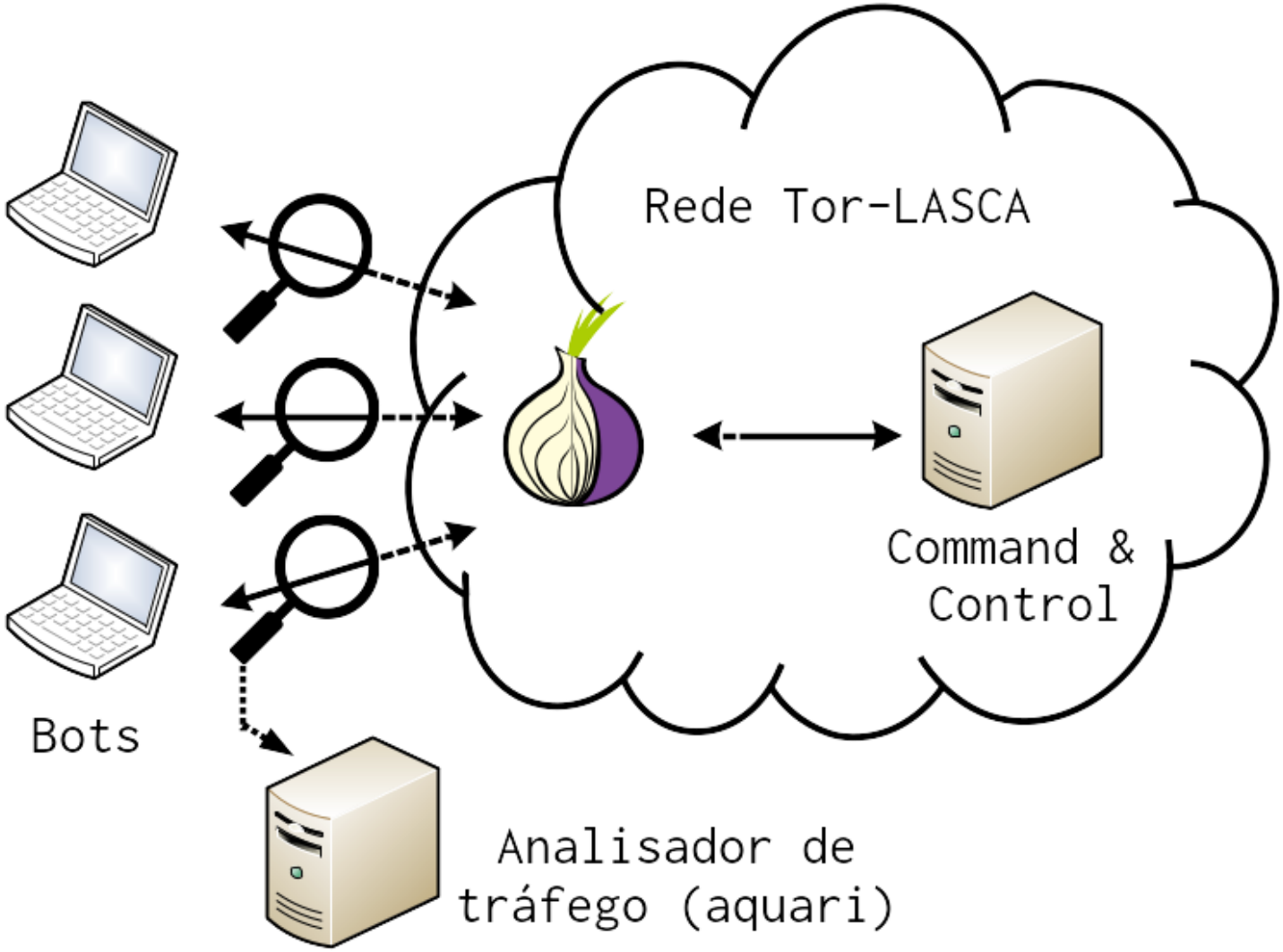
Como funciona uma botnet ***com Tor?***



UNICAMP

frida una iniciativa de LACNIC

OnionBots



UNICAMP

frida
una iniciativa
de LACNIC

Referências

1.Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router*. Naval Research Lab Washington DC.

2.Ling, Z., Luo, J., Wu, K., Yu, W., & Fu, X. (2014, April). TorWard: Discovery of malicious traffic over Tor. In INFOCOM, 2014 Proceedings IEEE (pp. 1402-1410). IEEE.

3.Tor metrics. https://metrics.torproject.org/, 2015.

4.Owen, G., & Savage, N. (2016). Empirical analysis of Tor hidden services. IET Information Security, 10(3), 113-118.

5.Casenove, M., & Miraglia, A. (2014, June). Botnet over Tor: The illusion of hiding. In Cyber Conflict (CyCon 2014), 2014 6th International Conference On (pp. 273-282). IEEE.

6.https://research.torproject.org/

7.Stone-Gross, et al. Your botnet is my botnet: analysis of a botnet takeover.

UNICAMP

frida una iniciativa de LACNIC

Obrigado!