Cibercrime

Instrumentos do Cibercrime

Seminário

2019

Nuno Santos

TÉCNICO LISBOA

Cibercrime

- **"Todo e qualquer acto ilegal envolvendo um computador, os seus sistemas, ou as suas aplicações"** (EC-Council)
  - EC-Council: International Council of Electronic Commerce Consultants
- Compreende um conjunto de delitos definidos em leis como:
  - The U.S. Computer Fraud
  - The UK Computer Abuse Act
  - Lei do Cibercrime, in Portugal

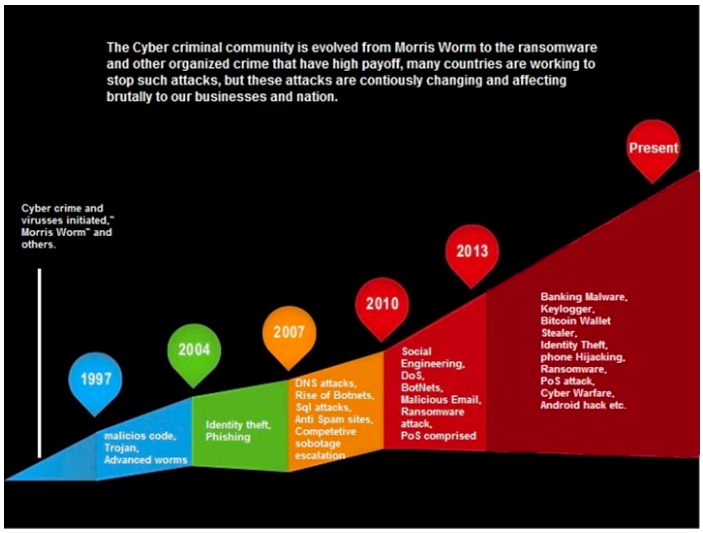
Exemplos de cibercrime

- Roubo de propriedade intelectual
- Roubo de identidade
- Fraude de identidade
- Fraude financeira
- Cyberbullying e cyberstalking
- Pornografia infantil
- Ciber extorsão
- Ataques de negação de serviço
- Intrusão em sistemas
- Instalação de programas maliciosos (malware)

Cibercrime in Portugal: Lei do Cibercrime

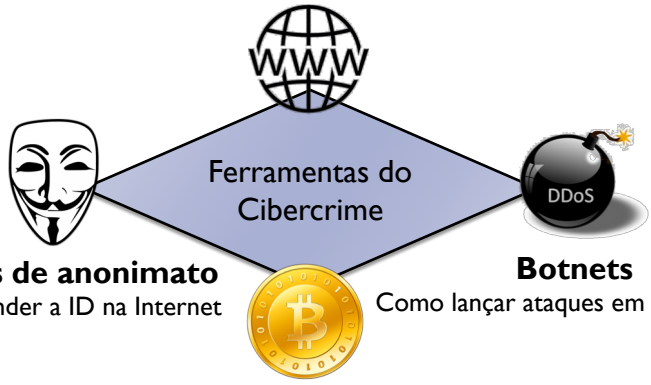
- Lei n.º 109/2009, de 15 de Setembro
  - http://goo.gl/PTg2oj
- CAPÍTULO II: Disposições penais materiais
  - Artigo 3.º: Falsidade informática
  - Artigo 4.º: Dano relativo a programas ou outros dados informáticos
  - Artigo 6.º: Acesso ilegítimo
  - Artigo 8.º: Reprodução ilegítima de programa protegido

Evolução do cibercrime



Principais instrumentos do cibercrime

Deep Web
Como encontrar informação e localizer serviços



Sistemas de anonimato
Como esconder a ID na Internet

Botnets
Como lançar ataques em larga escala

Criptomoeda
Como tornar os pagamentos não rastreáveis

TÉCNICO LISBOA

Deep Web

A Web: Recurso ponderoso para cibercriminosos

Cibercriminoso

- Oferece um gigantesto **repositório de informação,** usado em:
  - Premeditação de crimes, violações de privacidade, roubo de identidade, etc.
- Permite aceder a **serviços online** para actividade criminosa
  - Ex., venda de drogas, venda de armas, acesso a pornografia infantil, etc.
- Para encontrar esses recursos, existem poderosos **motores de busca**
  - Google, Bing, Shodan, etc.

A Web: recurso poderoso para investigadores

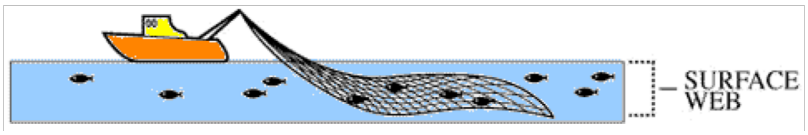
Investigadores

Google bing SHODAN Computer Search Engine

- Poderosa **ferramenta para investigação** de suspeitos
  - Provas em blogs, redes sociais, actividade de navegação web, etc.
- É a **arena** em que o próprio crime tem lugar
  - Transacções ilegais, cyber stalking, extorsão, fraude, etc.

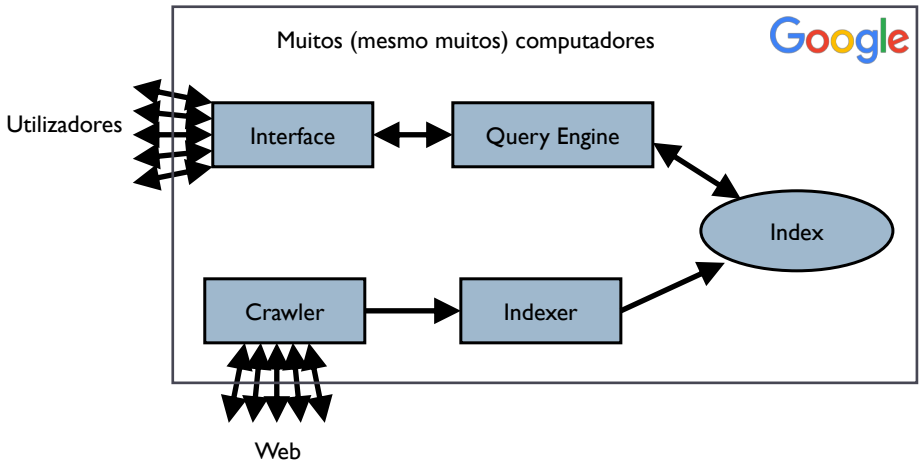
A Web e a analogia do iceberg

A Web de superfície

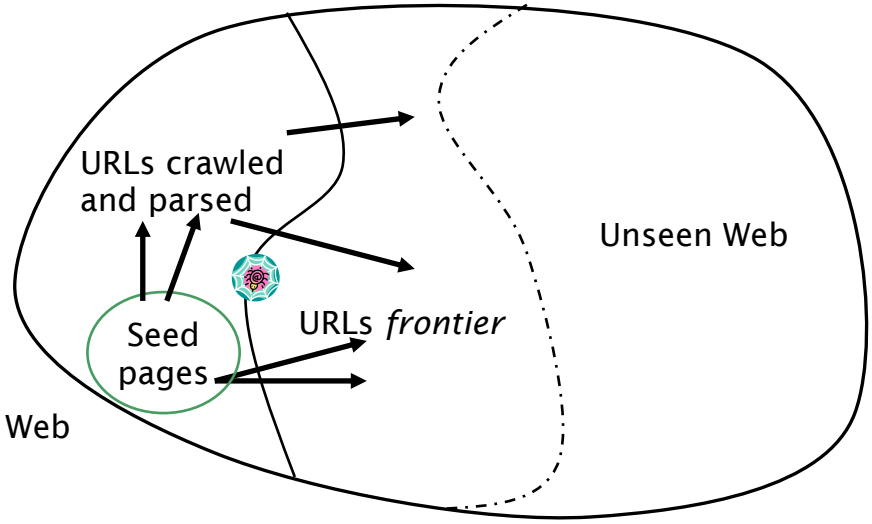


- **Surface Web:** Parte da Web acessível ao público em geral nos motores de busca convencionais
  - Outros nomes: Visible Web, Clearnet, Indexed Web, Indexable Web or Lightnet
- Em Junho, 2015, o índice da surface web criado pela Google continha cerca de 14.5 biliões de páginas

Como funciona um motor de busca convencional



Crawling da Web: A partir de páginas seminais



Google hacking

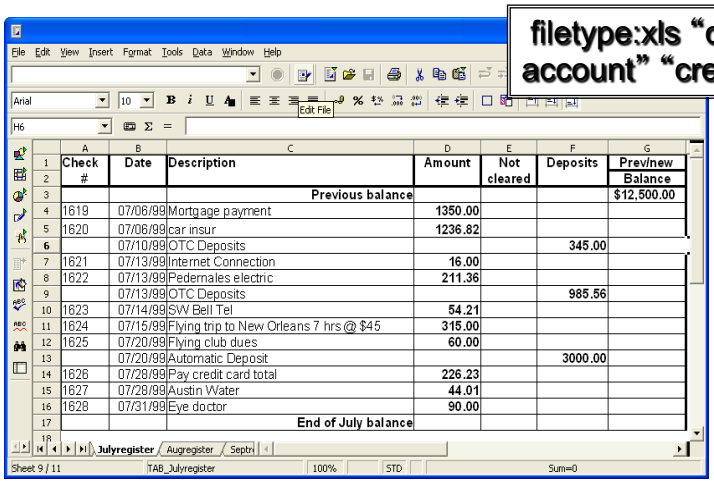
- Google oferece keywords para procuras avançadas
  - Operadores lógicos em expressões de pesquisa
  - Atributos avançados de pesquisa: **"login password filetype:pdf"**
- Para saber mais:
  - http://www.mrjoeyjohnson.com/Google.Hacking.Filters.pdf

Operator	Purpose
intitle	Search page Title
allintitle[3]	Search page title
inurl	Search URL
allinurl	Search URL
filetype	specific files
intext	Search text of page only
allintext	Search text of page only
site	Search specific site
link	Search for links to pages
inanchor	Search link anchor text
numrange	Locate number
daterange	Search in date range
author	Group author search
group	Group name search
insubject	Group subject search
msgid	Group msgid search

Exmplos: Pesquisar tipos de ficheiros sensíveis

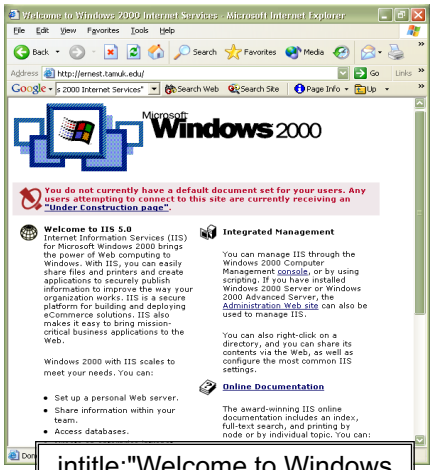
- filetype: restringe pesquisas ao tipo de ficheiro

filetype:xls "checking account" "credit card"

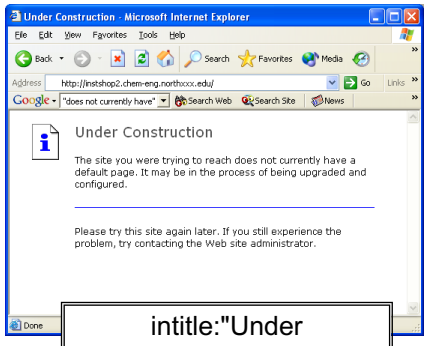


	A	B	C	D	E	F	G
1	Check #	Date	Description	Amount	Not cleared	Deposits	Prev/new Balance
2			Previous balance				$12,500.00
3	1619	07/06/99	Mortgage payment	1350.00			
4	1620	07/06/99	car insur	1236.82			
5		07/10/99	OTC Deposits			345.00	
6	1621	07/13/99	Internet Connection	16.00			
7	1622	07/13/99	Pedernales electric	211.36			
8		07/13/99	OTC Deposits			985.56	
9	1623	07/14/99	SW Bell Tel	54.21			
10	1624	07/15/99	Flying trip to New Orleans 7 hrs @ $45	315.00			
11	1625	07/20/99	Flying club dues	60.00			
12		07/20/99	Automatic Deposit			3000.00	
13	1626	07/28/99	Pay credit card total	226.23			
14	1627	07/28/99	Austin Water	44.01			
15	1628	07/31/99	Eye doctor	90.00			
16			End of July balance				

Exemplo: Encontrar servidores expostos



intitle:"Welcome to Windows 2000 Internet Services"



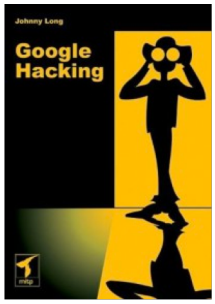
intitle:"Under construction" "does not currently have"

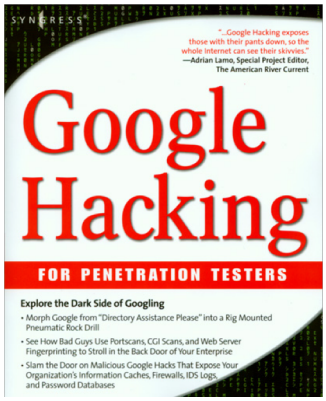
Exemplo: Encontrar webcams expostas

- Para encontar webcams não proteginas na Internet, usar a pesquisa seguinte:
  - inurl:/view.shtml

- Também é possível restringir por padrões de URL específicos do fabricante ou modelo
  - inurl:ViewerFrame?Mode=
  - inurl:ViewerFrame?Mode=Refresh
  - inurl:axis-cgi/jpg
  - ...

Google hacking: Livros inteiros sobre isto





Dornfest, Rael,* Google Hacks 3rd ed, *O'Rielly, (2006)

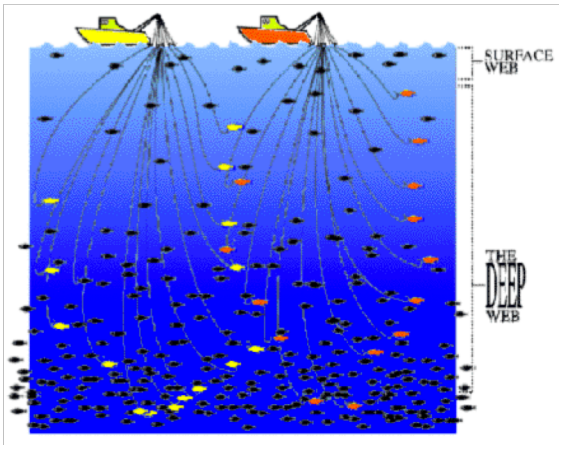
Ethical Hacking, http://www.nc-net.info/2006conf/Ethical_Hacking_Presentation_October_2006.ppt

A cheat sheet of Google search features:
http://www.google.com/intl/en/help/features.html

A Cheat Sheet for Google Search Hacks -- how to find information fast and efficiently
http://www.expertsforge.com/Security/hacking-everything-using-google-3.asp

Deep Web

- Parte da Web que não é indexada por motores de busca convencionais, logo não aparece nos resultados
- Porque não é indexado pelos motores de busca típicos?



Há conteúdo que não pode ser encontrado seguindo os URL

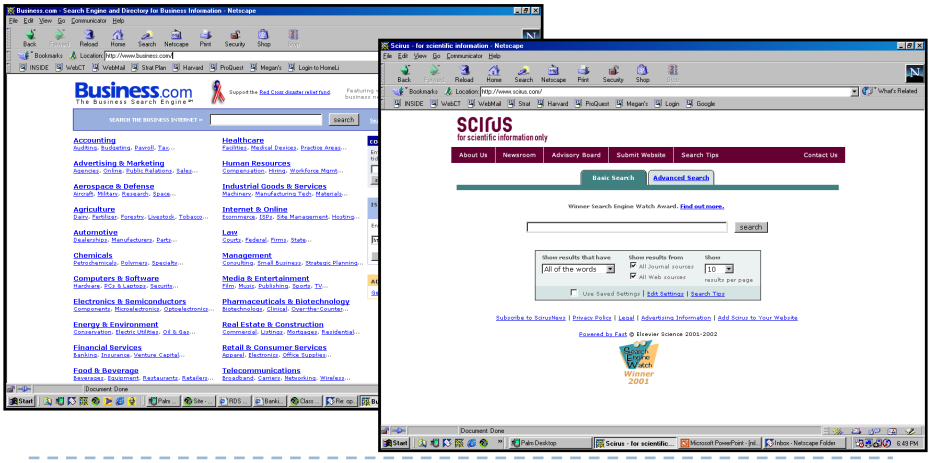
- Páginas dinâmicas e buscas em bases de dados
  - Resposta a pesquisas ou acedidas através de formulários
- Conteúdos não referenciados (unlinked)
  - Páginas sem links para elas (orfãs)
- Web privada
  - Sites que precisam de registo e login
- Web de acesso limitado
  - Sites com captchas, cabeçalhos http no-cache pragma

Noutros casos não dá para seguir o URL

- Restrições de crawling pelo dono do site
  - Usa ficheiro robots.txt para limitar indexação das páginas
- Restrições de crawling pelo motor de busca
  - Ex.: uma página pode estar neste URL:
    http://www.website.com/cgi-bin/getpage.cgi?name=sitemap
  - Muitos motores de busca não lêem depois do ?
- Limitações do motor de crawling
  - Ex., dados em tempo real – muda muito rapidamente

Motores de busca especializados

- Centenas de motores de busca para todos os tópicos



Um motor de busca especialmente interessante

SHODAN
Computer Search Engine

- Shodan permite pesquisar por **tipos específicos** de computadores ligados à Internet
  - Routers, servidores, semáforos, câmaras de vigilância, sistemas de aquecimento para casas
  - Sistemas de controlo de estações de serviço, tratamento de águas, parques aquáticos, redes eléctricas, centrais nucleares, aceleradores de partículas
- Porque é que é interessante?
  - Muitos dispositivos usam "admin" como username e "1234" como password, e só precisam de um browser para serem contactados

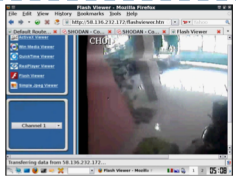
Como é que o Shodan funciona?

*"Google crawls URLs – I don't do that at all.The only thing I do is **randomly pick an IP** out of all the IPs that exist, whether it's online or not being used, and I **try to connect** to it on different ports. It's probably not a part of the visible web in the sense that you can't just use a browser. It's not something that most people can easily discover, just because it's not visual in the same way a website is."*

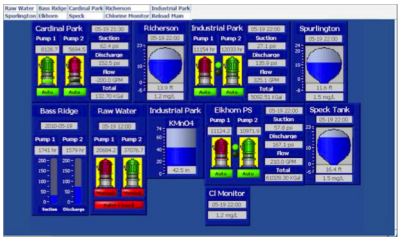
John Matherly, Shodan's creator

- Recolhe dados sobretudo de servidores HTTP (porto 80)
  - Mas também FTP (21), SSH (22) Telnet (23), and SNMP (161)

Coisas surpreendentes que podemos encontrar

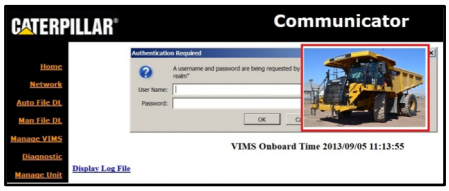


Webcam



Controlos para tratamento de águas

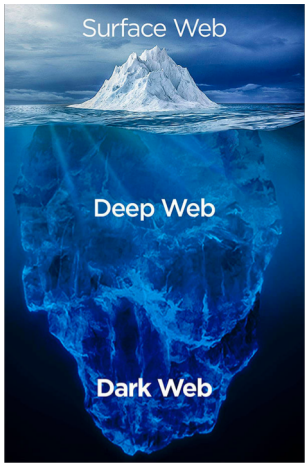
Controlos de um crematório



Controlos de camiões

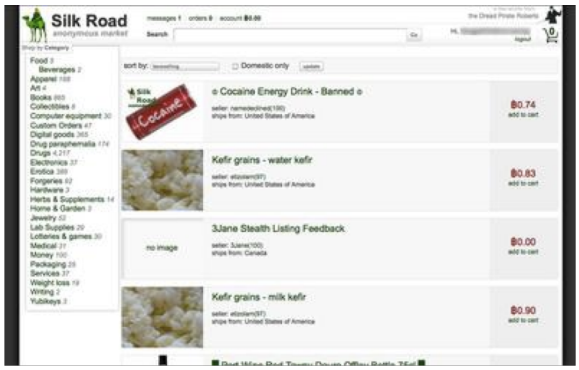
Mais no fundo encontramos a Dark Web

- **Dark Web** constiste em conteúdos que existem em darknets
- **Darknets** são redes próprias na Internet que requerem software específico para acesso e oferecem propriedades de anonimato
  - Montadas em redes peer-to-peer
  - Como hidden services sobre o Tor



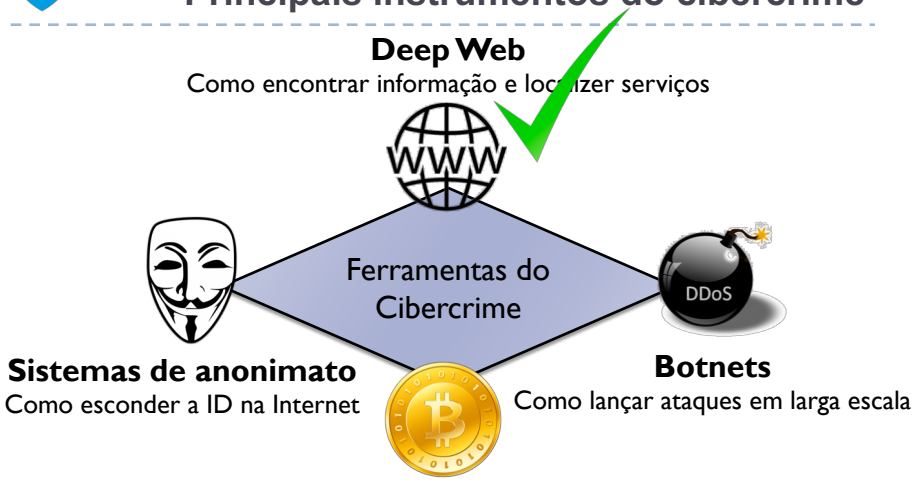
Dark Web: marketplace de actividades ilícitas

- Serviços de piratearia informática
- Serviços para realização de fraude e lavagem de dinheiro
- Mercados de produtos ilegais (armas, drogas)
- Pornografia infantil
- Assassinos profissionais
- …



Principais instrumentos do cibercrime

Deep Web
Como encontrar informação e localizar serviços



Sistemas de anonimato
Como esconder a ID na Internet

Botnets
Como lançar ataques em larga escala

Criptomoeda
Como tornar os pagamentos não rastreáveis

TÉCNICO LISBOA

Anonimato online

Porquê ser anónimo na Internet?

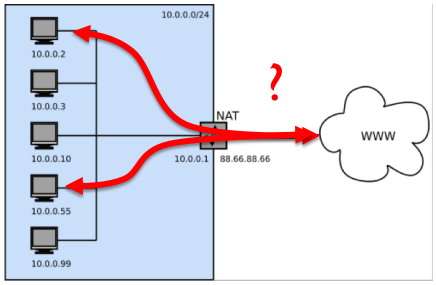
- Se for um cibercriminoso!
  - Infractor de direitos de autor, pirata, spammer, terrorista, etc.
- Mas também se for:
  - Jornalista
  - Whistleblower
  - Activista de direitos humanos
  - Quadros executivos
  - Militares e agências de intelligence
  - Vítima de abuso

Na Internet é difícil ser totalmente anónimo

- O teu **endereço IP** pode ser relacionado contigo
  - Os ISPs guardam registos das comunicações
  - Durante alguns anos (Data Retention Laws)
  - Esses registos podem ser obtidos por ordem judicial
- O teu **browser** pode ser identificado e rastreado
  - Cookies, Flash cookies, HTML5 storage
  - Browser fingerprinting
- As tuas **actividades** online podem identificar-te
  - Os sites web e apps únicos que usas
  - O tipo de links a que acedes

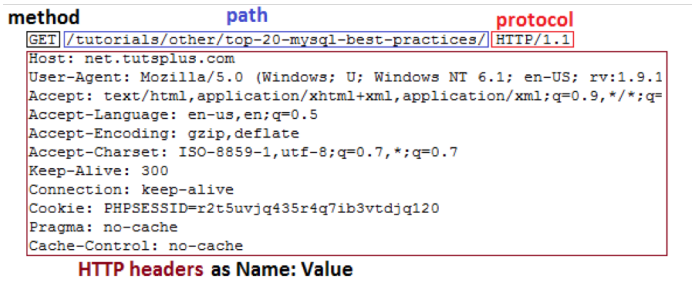
Exemplo da dificuldade de ser anónimo

- A NAT esconde múltiplos clientes por detrás do mesmo IP
- Como identificar esses clientes?
  - Se tiveres acesso à NAT, consultar a tabela de mapeamento
  - Caso contrário?...

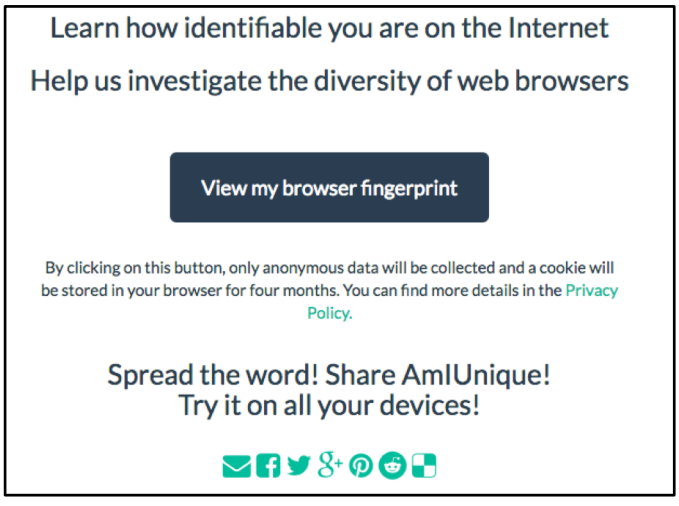


Browser fingerprinting

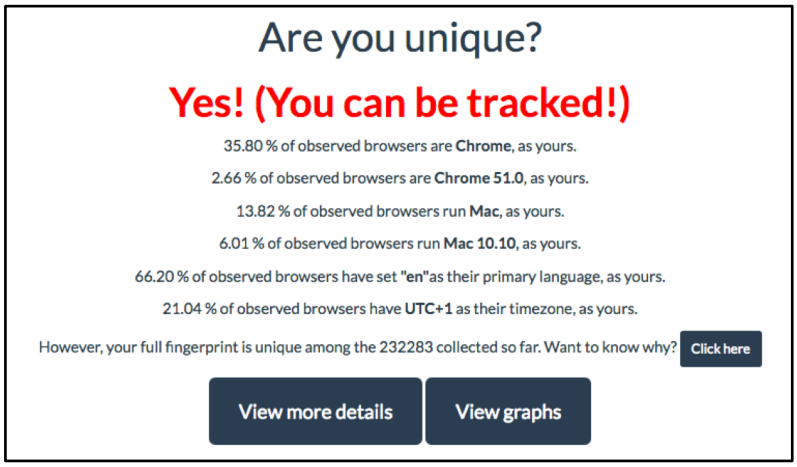
- Recolha sistemática de informação sobre o browser
  - Pedido HTTP (user agent e accept headers)
  - Javascript API (ex.., plugins installados)
  - Flash plugin API (e.g., versão OS, lista de fontes, resolução de ecrã)
  - Elemento HTML5 Canvas (differenças em image rendering)



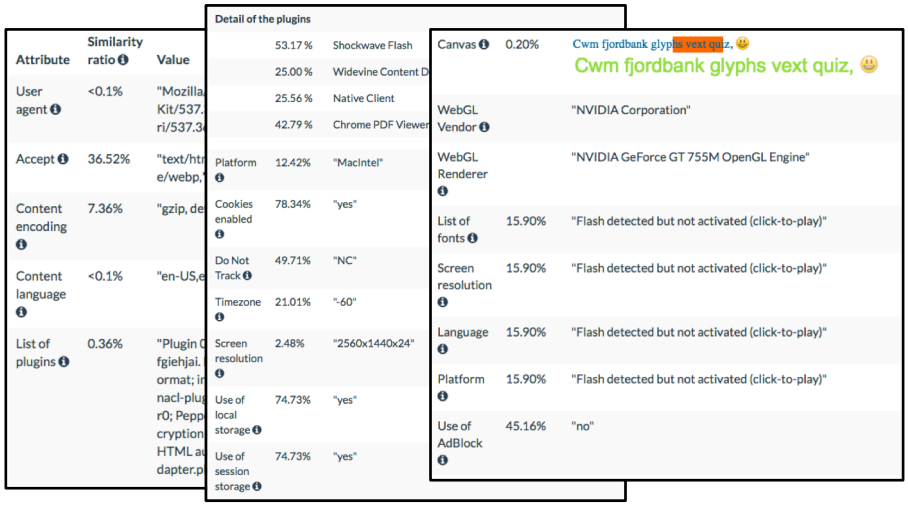
http://amiunique.org



Results on my browser

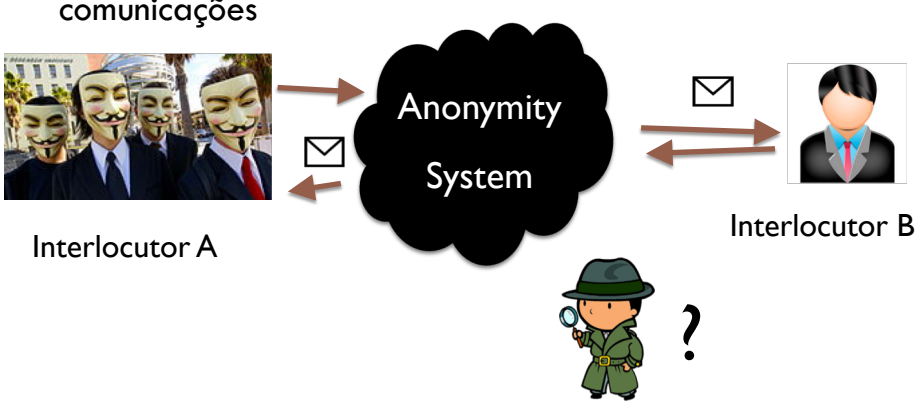


Perceber os detalhes desta identificação



Anonymity systems

- Procuram ocultar a identidade dos interlocutores das comunicações



Tipos de anonimato

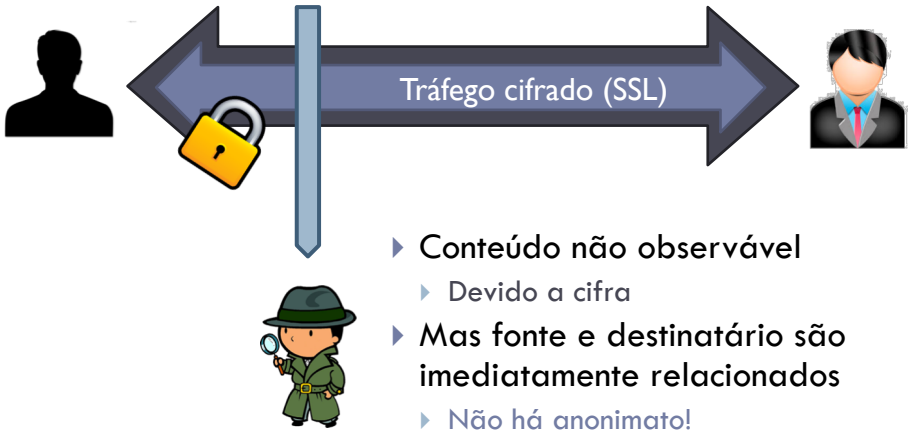
- **Anonimato do remetente**
  - Não se consegue dizer quem enviou a mensagem
- **Anonimato do destinatário**
  - Não se consegue dizer quem recebeu a mensagem
- **Anonimato do remetente e destinatário**
  - Não se consegue dizer se A e B são o remetente e destinatário da mensagem

Quantificar o anonimato

- Como quantificar o quão anónimos estamos?
  - **Conjuntos de anonimato**

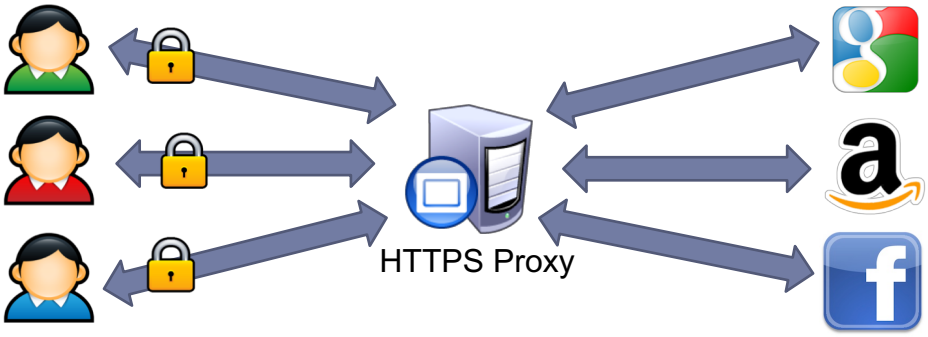
- Quanto maior o conjunto = mais forte o anonimato

Exemplo em que não existe anonimato



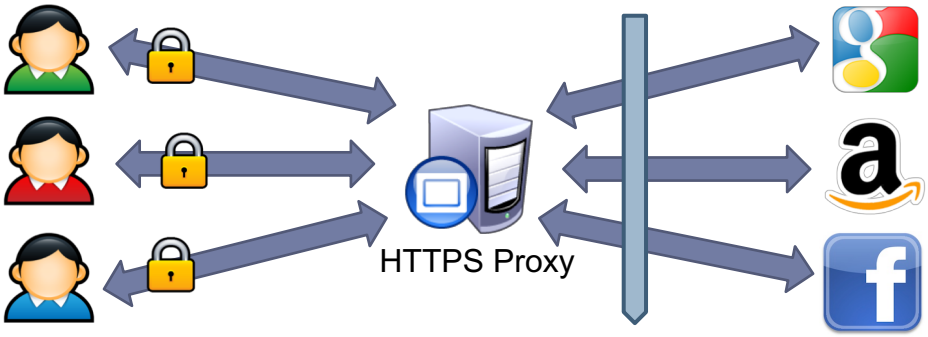
- Conteúdo não observável
  - Devido a cifra
- Mas fonte e destinatário são imediatamente relacionados
  - Não há anonimato!

Abordagem básica: Proxies de anonimização



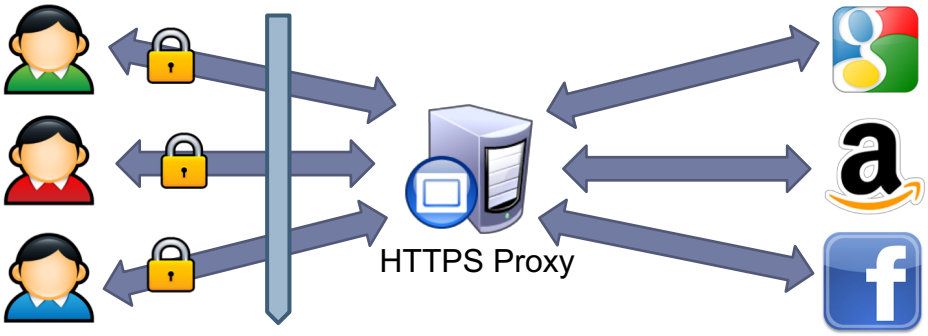
Web proxies reencaminham tráfego HTTPS traffic
ex., https://www.anonymizer.com, http://www.bind2.com/

Investigação de proxies de anonimato



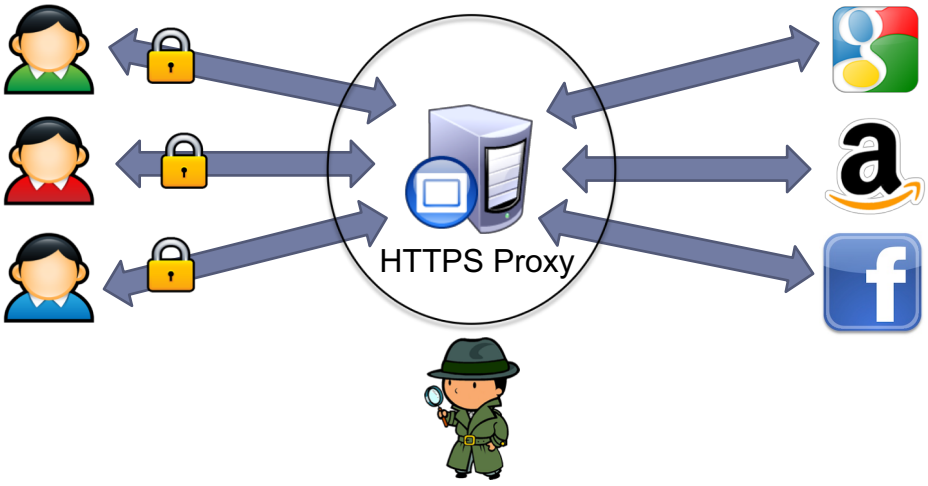
- O destino é conhecido
- Anonimato do remetente

Investigação de proxies de anonimato



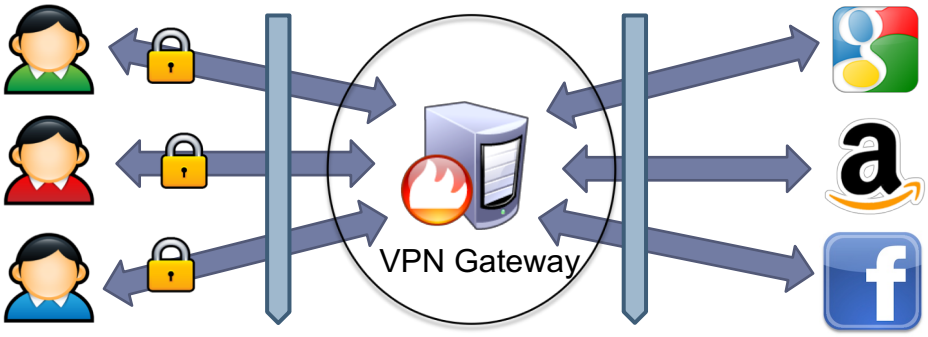
- Remetente é conhecido
- Anonimato do destinatário

Investigação de proxies de anonimato



Não há anonimato

Mesmas propriedades para qualquer proxy



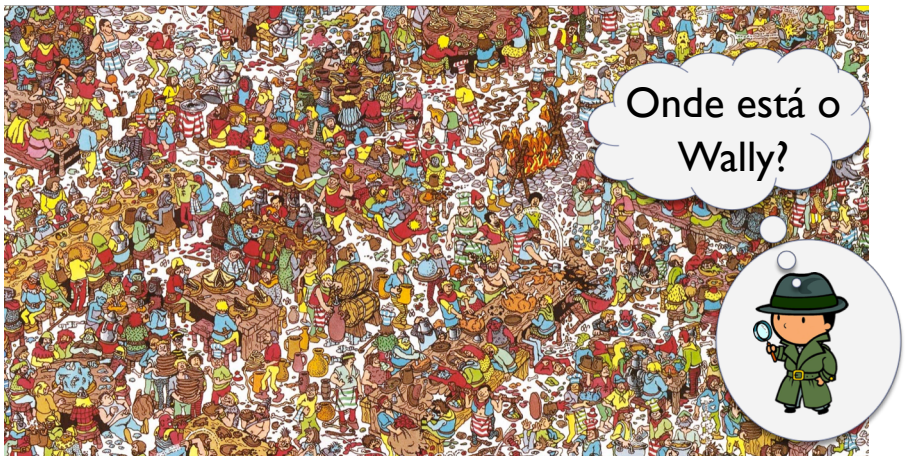
- Remetente é conhecido
- Anonimato do destinatário

- O destino é conhecido
- Anonimato do remetente

Não há anonimato

Aumentar protecção: Anonimato adora companhia

Mecanismo chave: misturar-se na multidão

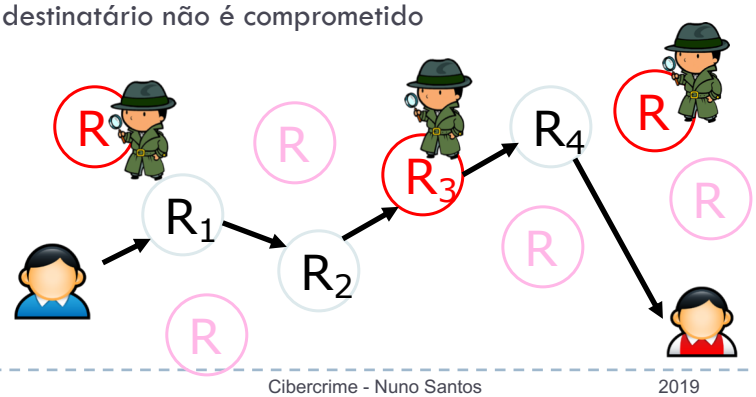


Rede de anonimato

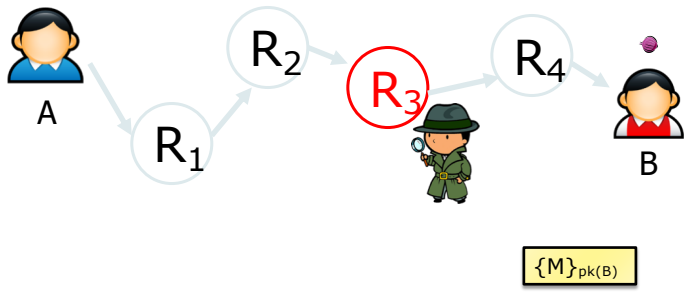
- Ultrapassa limitações do proxy server, onde…
  - O detentor do proxy pode ser forçado a revelar os logs
  - Pior, pode mesmo ser um honeypot
- **Rede de anonimato**: encaminha tráfego através de uma cadeia de nós da rede chamados **relays**
  - Redes de anonimato popupares: Tor, I2P
- Tor incorpora algumas ideias de **onion routing**

Protocolos de onion routing

- Utilizador estabelece um circuito entre nós da rede (relays) de anonimato
- Protocolo de segurança garante que mesmo que um dos relays seja comprometido, o anonimato remetente-destinatário não é comprometido

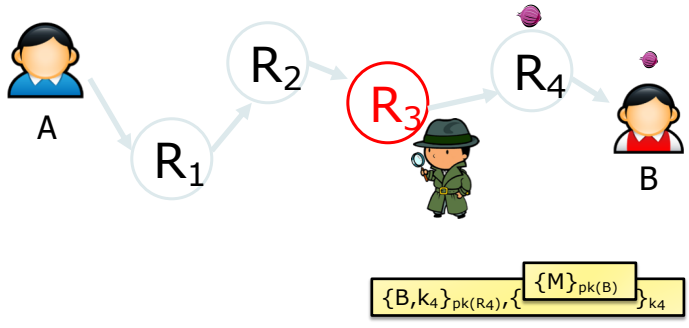


Estabelecimento do caminho



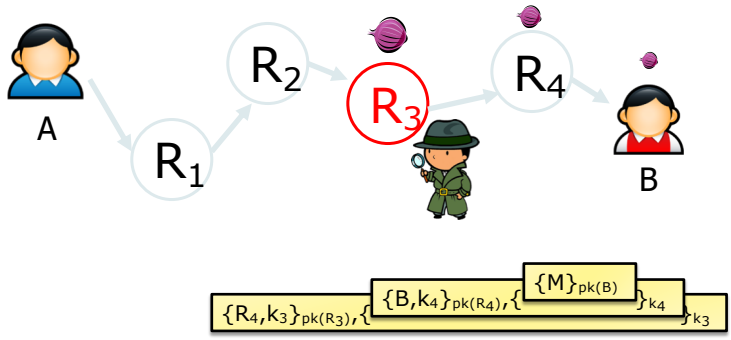
- Informação de routing em cada link cifrada com a chave publica do respective relay
- Cada relay aprende apenas o próximo relay do circuito

Route establishment in basic onion routing



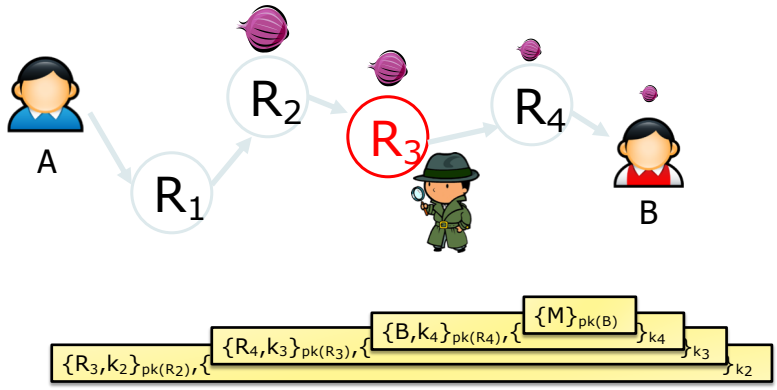
- Informação de routing em cada link cifrada com a chave publica do respective relay
- Cada relay aprende apenas o próximo relay do circuito

Route establishment in basic onion routing



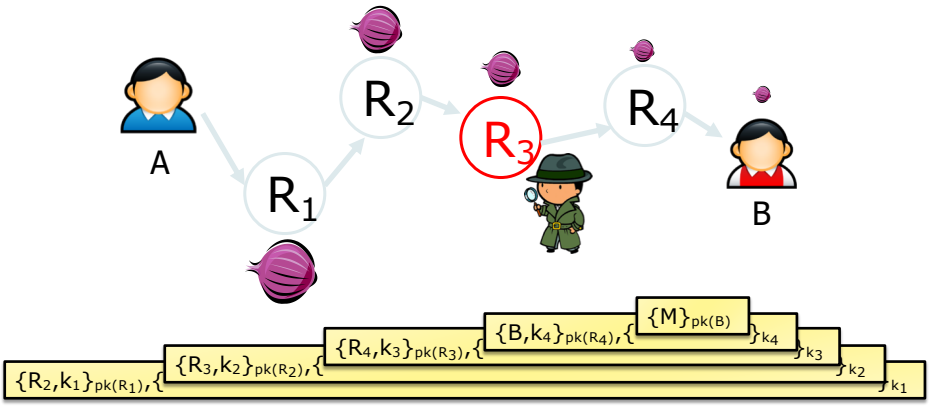
- Informação de routing em cada link cifrada com a chave publica do respective relay
- Cada relay aprende apenas o próximo relay do circuito

Route establishment in basic onion routing



- Informação de routing em cada link cifrada com a chave publica do respective relay
- Cada relay aprende apenas o próximo relay do circuito

Route establishment in basic onion routing

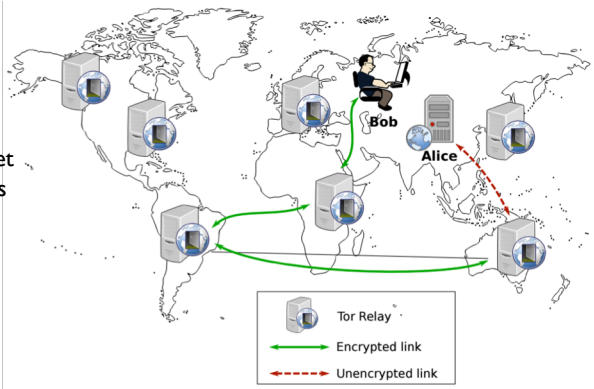


- Informação de routing em cada link cifrada com a chave publica do respective relay
- Cada relay aprende apenas o próximo relay do circuito

Tor: A 2ª geração de onion routing

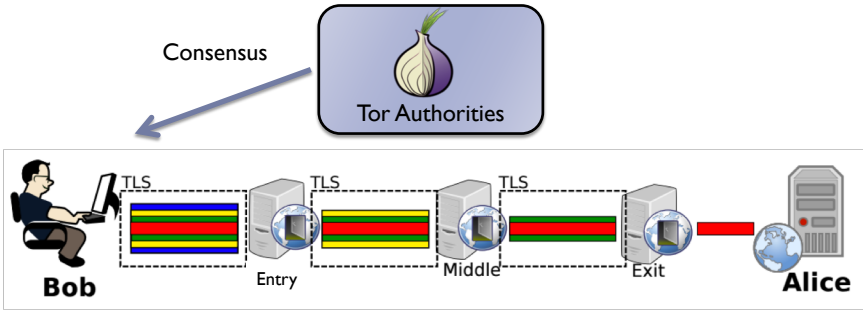
- **Tor** é uma rede de anonimato de baixa latência para comunicações na Internet

Using Tor makes it more difficult for non-global adversaries to trace Internet activity for TCP applications



Tor circuit

- O Bob escolhe três relays do directório (consensus)
- A Tor client builds a circuit one hop at a time

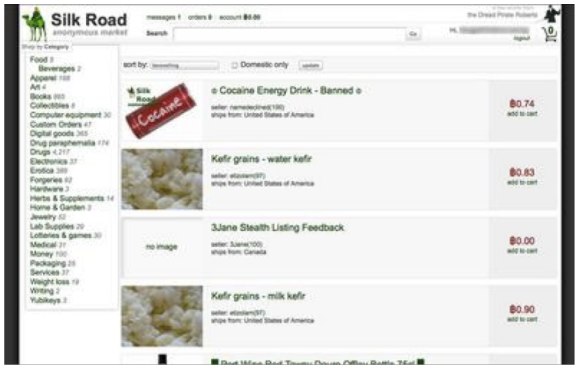


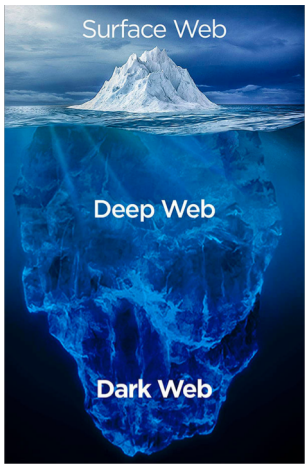
Layered encryption

Serviços ocultos

- Tor esconde o remetente, mas o destinatário é exposto
- E se o criminoso pretende ter um serviço web anonimo?
  - Ou seja, um site em que ninguém sabe o IP do servidor web?
- Tor tem uma resposta: **serviços ocultos**
  - Permite correr um servidor e permitir que clientes se conectem sem revelar o IP ou o nome DNS
- Muitos serviços ocultos
  - Tor Mail, Tor Char
  - DuckDuckGo
  - The Pirate Bay
  - Silk Road (2.0)

Tor e serviços ocultos estão na base da Dark Web





Principais instrumentos do cibercrime

Deep Web
Como encontrar informação e localizar serviços

Ferramentas do Cibercrime

Sistemas de anonimato
Como esconder a ID na Internet

Botnets
Como lançar ataques em larga escala

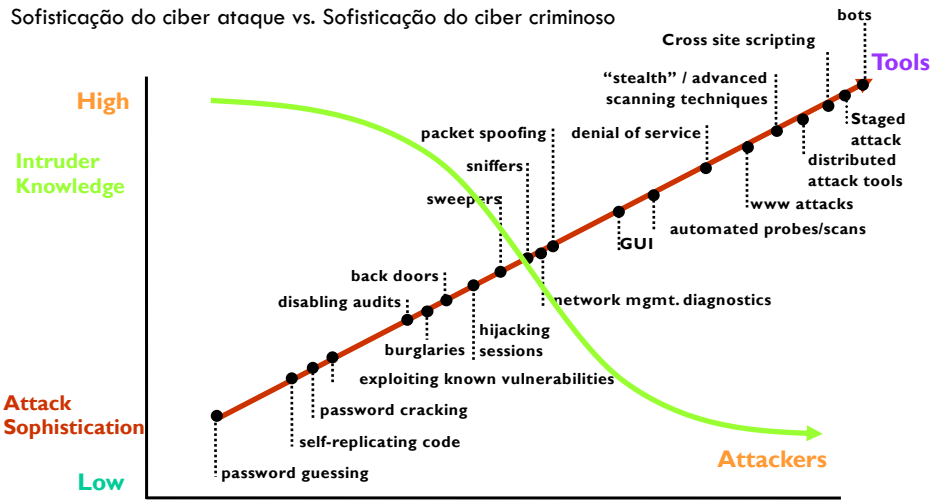
Criptomoeda
Como tornar os pagamentos não rastreáveis

TÉCNICO LISBOA

Botnets

Botnets: ameaças de segurança

Sofisticação do ciber ataque vs. Sofisticação do ciber criminoso

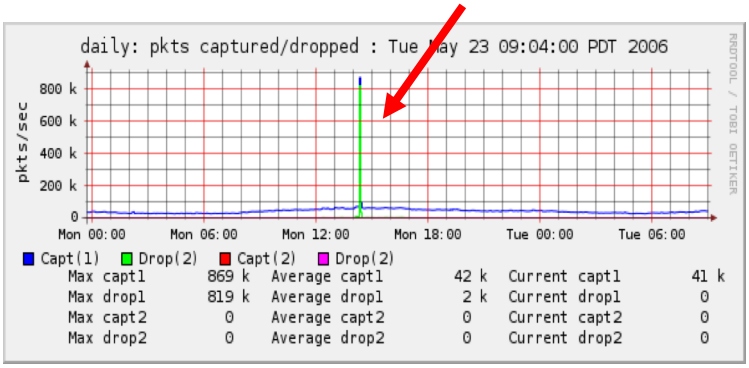


O que é uma botnet?

- **Botnet:** colecção de "robots" em software que se executam em computadores de forma autónoma e automaticamente, e que são controlados remotamente por um ou mais atacantes
- Armas online muito eficazes para terrorismo
  - Ou seja, permitem realizar ataques a infrastruturas e estados
- Um dos meios principais para actividade maliciosa

Ataques Distributed Denial-of-Service (DDoS)

- Objectivo: inundar uma máquina vítima e negar serviço a clients legítimos
- Aqui estamos sob ataque!



Ataques DDoS no mundo real

Security

Massive DDoS racks up $30,000-a-day Amazon bill for China activists

Site flooded with 2.6 billion requests an hour

WEB NEWS 27/01/2015

Facebook: down and out again (along with Instagram) after DDoS attack?

By Darren Allan, CONTRIBUTING EDITOR

From the Twitter blog:

GitHub Status @githubstatus · Oct 22

We're investigating what appears to be a DDoS attack.

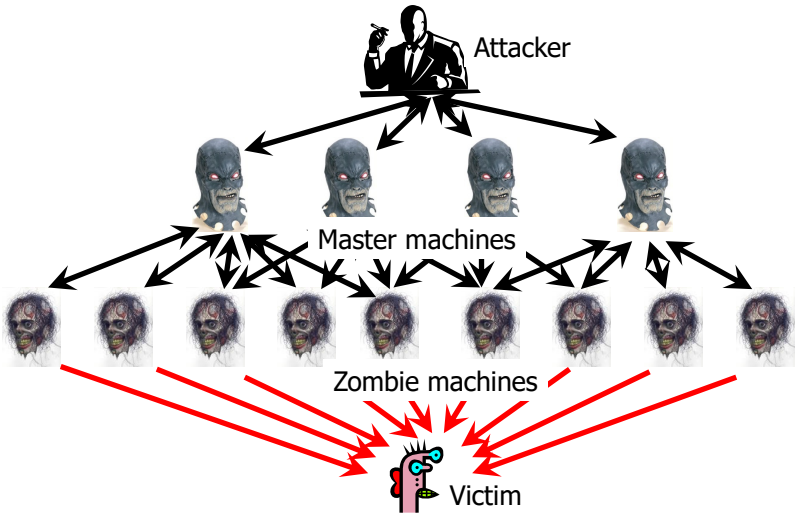
51 18 •••

ProtonMail still under attack by DDoS bombardment

November 5, 2015 - admin - 0 Comment

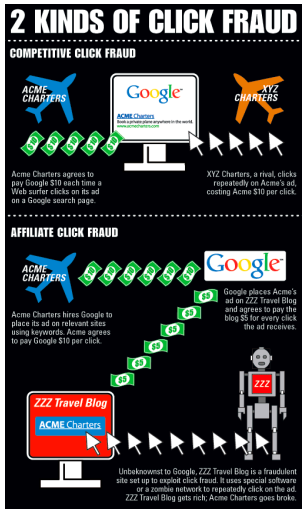
Secure webmail outfit ProtonMail is still fighting against a sustained DDoS attack that has left its service largely unavailable since Tuesday. In a statement posted to a hastily erected blog site, ProtonMail said the powerful attack by unknown parties has also inflicted collateral damage on third-party organisations. The attackers began by flooding our IP addresses. That quickly expanded to the…

Lançar ataques DDoS usando uma botnet



Botnet activities

- Ataques DDoS
- Roubo de dados
- Phishing
- Spam
- Click fraud
- Procura de vulnerabilidades
- …



Porque são instrumentos tão poderosos?

1. Grandíssima escala

- Milhares de milhões de zombies

Botnet	Estimated size
Conficker (2008)	10.500.000
BredoLab (2009)	30.000.000
Ramnit (2011)	3.000.000
Torpig	180.000
Storm	160.000
Asprox	15.000

2. Difícil de derrotar

- Zombies são parte da multidão

3. Fáceis de gerir

Quão fácil é construir uma botnet?

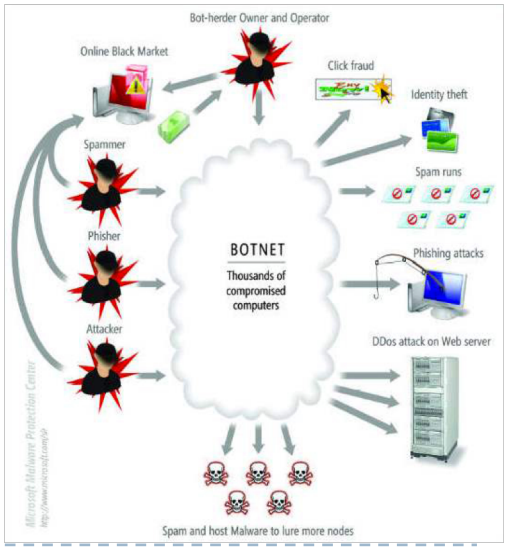
How To Build A Botnet In 15 Minutes

With a quick Google search and a little bit of time, nearly anyone can build their own botnet. Cry havoc!

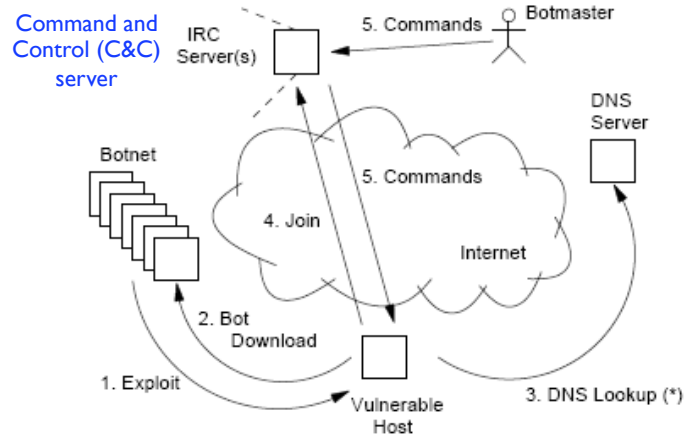
BRIAN PROFFITT · JUL 31, 2013

Botnet: Mercado global

- Botmasters não são os únicos beneficiários
- Quem paga:
  - Internet Advertising companies for downloading adware onto vulnerable PCs
  - Companies who send spam, viruses and other malware
  - …



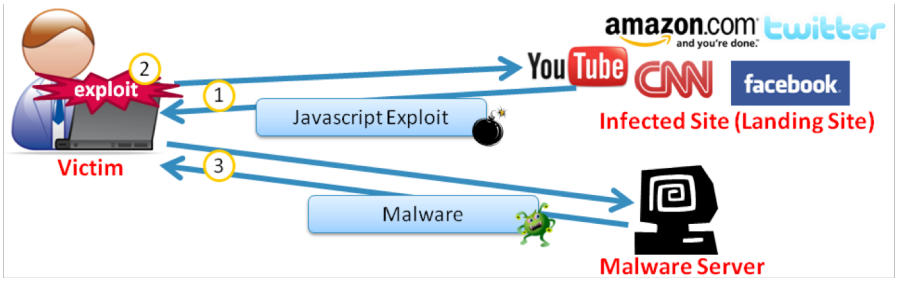
Recrutamente na botnet: The big picture



(*) : Optional Step

Métodos para infectar botnet nodes

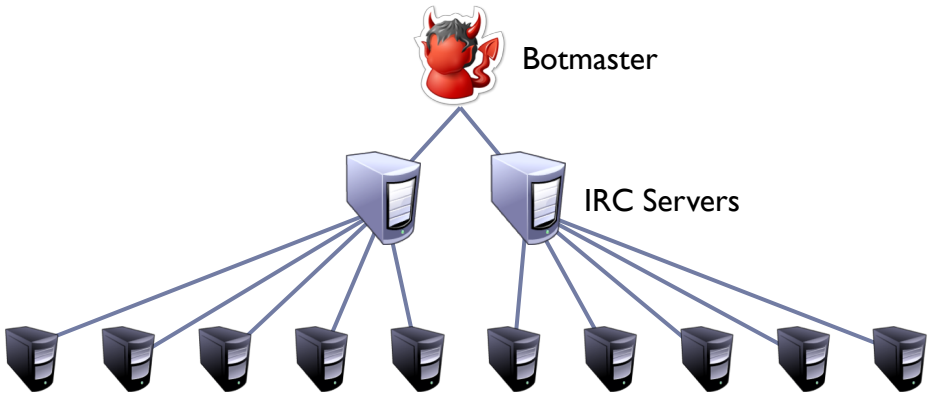
- Email
- Software pirateado
- Drive-by download



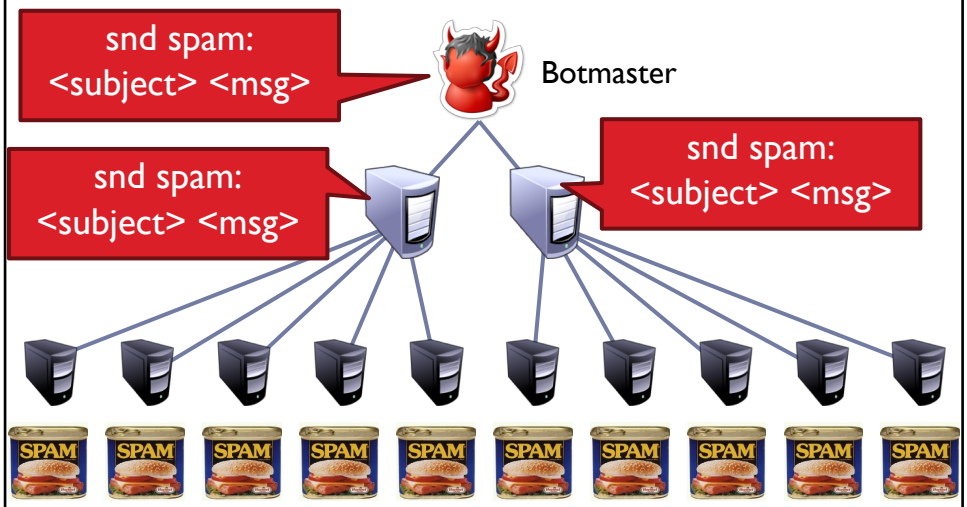
Técnicas de protecção das botnets

- Cifra
- Rootkits
- Tirar partido de protocolos e sistemas existentes
  - Ex., IRC, HTTP, etc.
- Fast Flux and Domain Generation Algorithms (DGA)
- Arquitecturas P2P

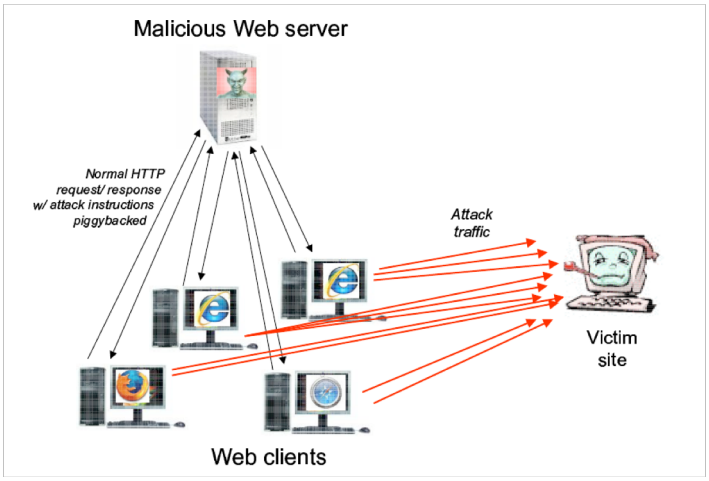
Arquitectura C&C centralizada



Arquitectura C&C centralizada: Canais IRC

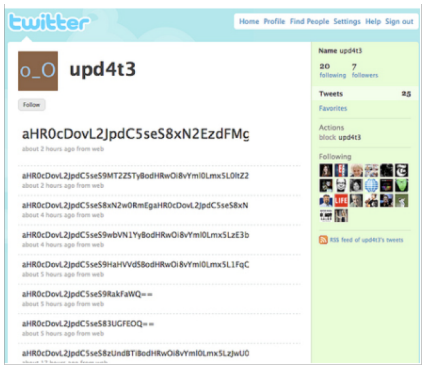


Usar HTTP



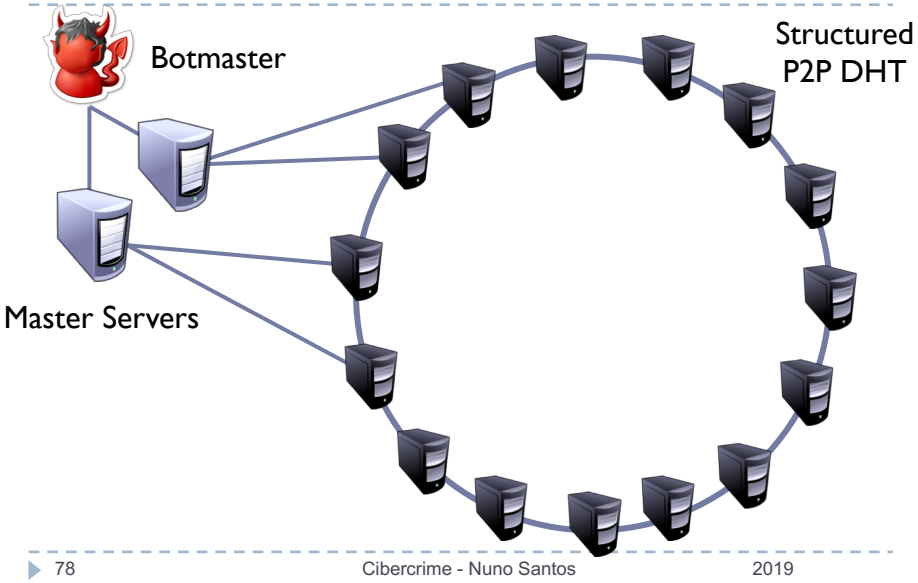
Serviços Web

- Redes sociais começam a ser usadas para controlo de botnets

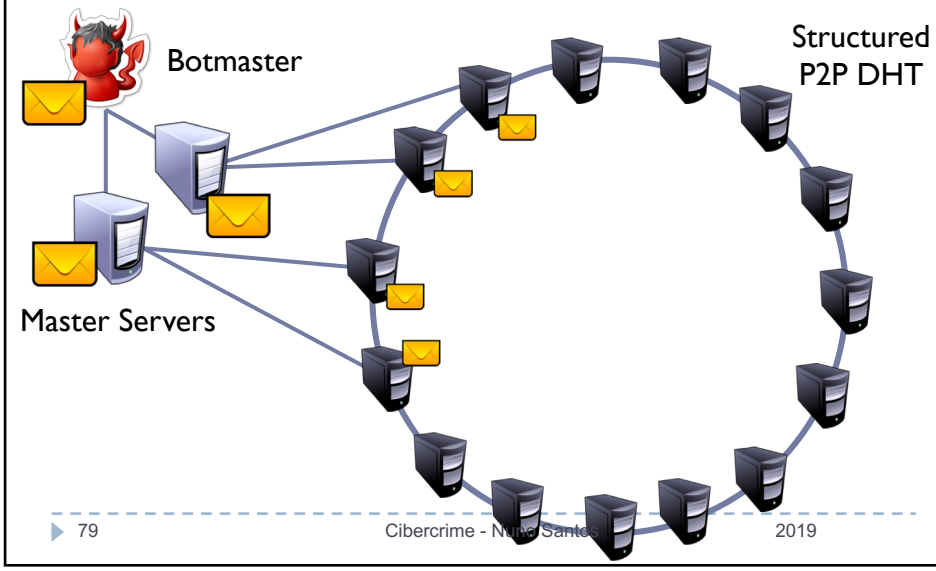


- Botnets começam a atingir sistemas industriais e móveis

P2P Botnets

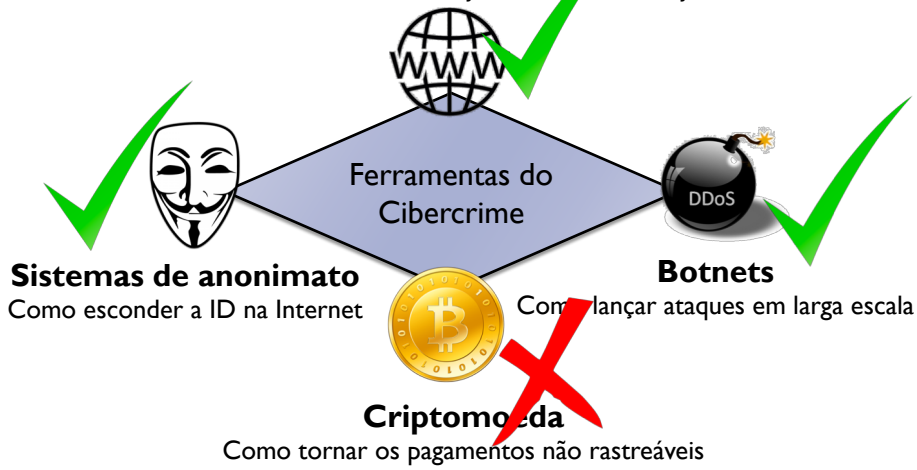


P2P Botnets



Principais instrumentos do cibercrime

Deep Web
Como encontrar informação e localizar serviços



Sistemas de anonimato
Como esconder a ID na Internet

Botnets
Como lançar ataques em larga escala

Criptomoeda
Como tornar os pagamentos não rastreáveis

Conclusions

- Botnets are amongst the most advanced tools for carrying out cybercrime (e.g., DDoS, data theft, spam)
- To evade detection, botnets employ highly sophisticated techniques, such as P2P architectures, fast flux, DGA, encryption, etc.
- Detecting and deterring botnets is a very challenging task and an active topic of security research

Conclusions

- Anonymity systems enable general users to preserve their privacy online, but can be used for criminal purposes
- Overtime, anonymity systems have evolved so much that that it is hard for forensic investigators to thwart them, notably Tor
- Despite the advanced techniques employed by these systems, however, there are weaknesses that allow for user de-anonymization techniques to be successfully employed

Conclusões

- O cibercrime tem evoluído dramaticamente nos últimos anos multiplicando-se em número e em variedade de actividades maliciosas
- Levar a cabo essas actividades é cada vez mais fácil de realizar impunemente e em larga escala devido à existência de instrumentos muito avançados
- Desses instrumentos e recursos destacamos quatro: a deep web, sistemas de anonimato, botnets, e criptomoeda