



Cibercrime

Instrumentos do Cibercrime

 TÉCNICO
LISBOA

Seminário

2019

Nuno Santos



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



▶ 2

Cibercrime - Nuno Santos

2019



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)

▶ 3

Cibercrime - Nuno Santos

2019



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

▶ 4

Cibercrime - Nuno Santos

2019



Evolução do cibercrime

The Cyber criminal community is evolved from Morris Worm to the ransomware and other organized crime that have high payoff, many countries are working to stop such attacks, but these attacks are contiously changing and affecting brutally to our businesses and nation.

Cyber crime and viruses initiated, "Morris Worm" and others.

1997
malicious code,
Trojan,
Advanced worms

2004
Identity theft,
Phishing

2007
DNS attacks,
Rise of Botnets,
Sql attacks,
Anti Spam sites,
Competitive
Market
escalation

2010

2013

Social
Engineering,
DoS,
Botnets,
Malicious Email,
Ransomware
attack,
PoS comprised

Present

Banking Malware,
Keylogger,
Bitcoin Wallet
Attack,
Identity Theft,
phone Hijacking,
Ransomware,
PoS attack,
Cyber Warfare,
Android hack etc.

▶ 5

Cibercrime - Nuno Santos

2019



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

▶ 6

Cibercrime - Nuno Santos

2019

Deep Web

7

Cibercrime - Nuno Santos

2019



A Web: Recurso ponderoso para cibercriminosos



Cibercriminoso



- ▶ Oferece um gigantesco **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.

▶ 8

Cibercrime - Nuno Santos

2019



A Web: recurso poderoso para investigadores



Investigadores



- ▶ 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.

▶ 9

Cibercrime - Nuno Santos

2019



A Web e a analogia do iceberg



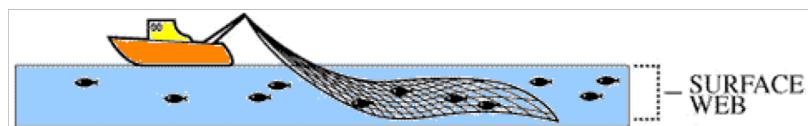
▶ 10

Cibercrime - Nuno Santos

2019



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

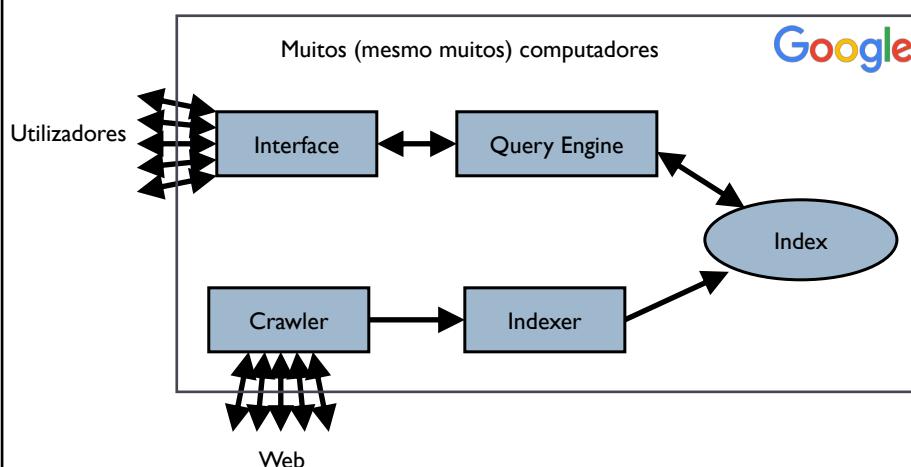
▶ 11

Cibercrime - Nuno Santos

2019



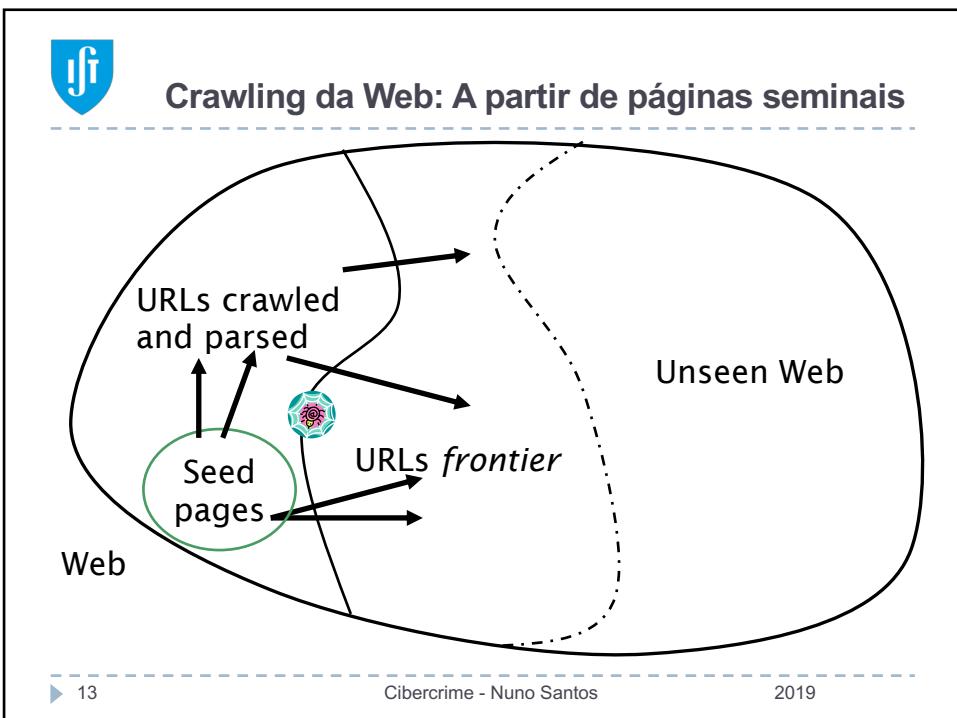
Como funciona um motor de busca convencional



▶ 12

Cibercrime - Nuno Santos

2019



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

Google hacking

- ▶ Google oferece keywords para procura 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>

▶ 14 Cibercrime - Nuno Santos 2019



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

► 15

Cibercrime - Nuno Santos

2019



Exemplo: Encontrar servidores expostos

intitle:"Welcome to Windows 2000 Internet Services"

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

► 16

Cibercrime - Nuno Santos

2019



Exemplo: Encontrar webcams expostas

- ▶ Para encontrar webcams não protegidas 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`
 - ▶ ...

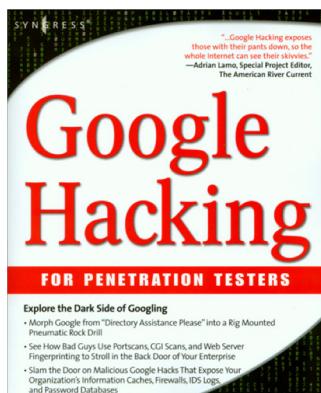
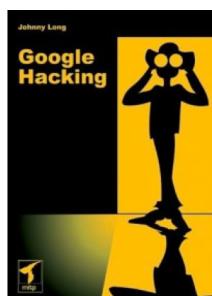
▶ 17

Cibercrime - Nuno Santos

2019



Google hacking: Livros inteiros sobre isto



Dornfest, Rael, **Google Hacks 3rd ed,**
O'Reilly, (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>

▶ 18

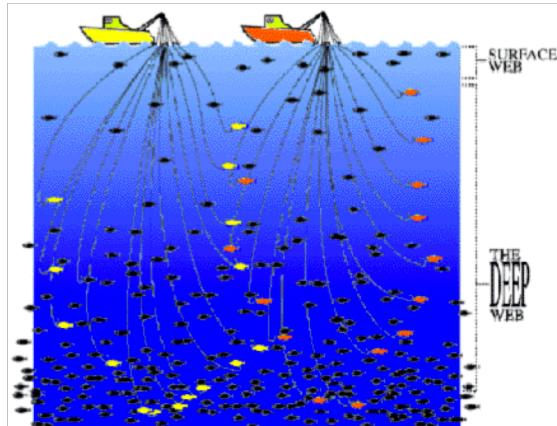
Cibercrime - Nuno Santos

2019



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?



▶ 19

Cibercrime - Nuno Santos

2019



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

▶ 20

Cibercrime - Nuno Santos

2019



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

► 21

Cibercrime - Nuno Santos

2019



Motores de busca especializados

► Centenas de motores de busca para todos os tópicos

The screenshot shows two side-by-side browser windows. The left window is for 'Business.com' and displays a search results page for 'Healthcare'. The right window is for 'SICRUS' and also displays a search results page for 'Healthcare'. Both pages show various links related to healthcare.

► 22

Cibercrime - Nuno Santos

2019



Um motor de busca especialmente interessante



- ▶ 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

▶ 23

Cibercrime - Nuno Santos

2019



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)

▶ 24

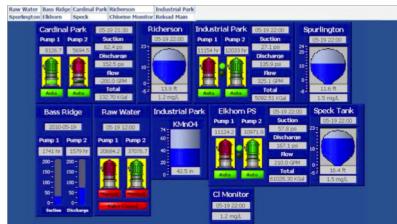
Cibercrime - Nuno Santos

2019

 Coisas surpreendentes que podemos encontrar



Webcam



Controlos para tratamento de águas



Controlos de um crematório



Controlos de camiões

▶ 25
Cibercrime - Nuno Santos
2019

 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

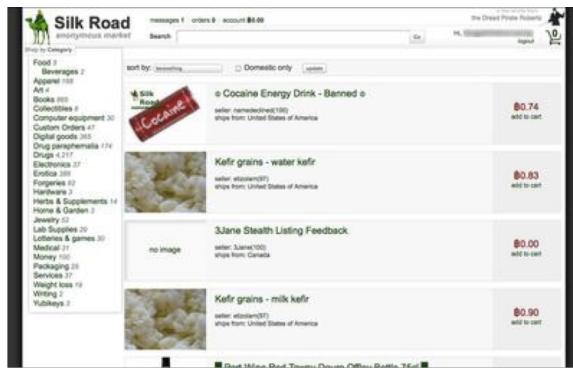


▶ 26
Cibercrime - Nuno Santos
2019



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
- ▶ ...



▶ 27

Cibercrime - Nuno Santos

2019



Principais instrumentos do cibercrime

Deep Web

Como encontrar informação e localizar serviços



Sistemas de anonimato

Como esconder a ID na Internet

Ferramentas do Cibercrime



Botnets

Como lançar ataques em larga escala



Criptomoeda

Como tornar os pagamentos não rastreáveis

▶ 28

Cibercrime - Nuno Santos

2019

Anonimato online

29

Cibercrime - Nuno Santos

2019



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

► 30

Cibercrime - Nuno Santos

2019



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 identificarte
 - ▶ Os sites web e apps únicos que usas
 - ▶ O tipo de links a que acedes

▶ 31

Cibercrime - Nuno Santos

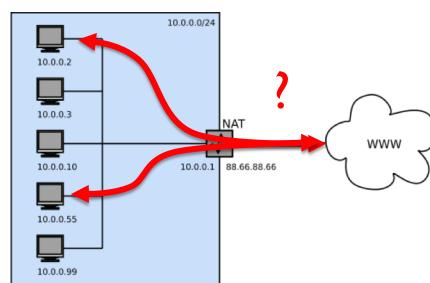
2019



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?...



▶ 32

Cibercrime - Nuno Santos

2019



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 (diferenças em image rendering)

method	path	protocol
GET	/tutorials/other/top-20-mysql-best-practices/	HTTP/1.1
Host:	net.tutsplus.com	
User-Agent:	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20100101 Firefox/4.0 (like Gecko)	
Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	
Accept-Language:	en-us,en;q=0.5	
Accept-Encoding:	gzip,deflate	
Accept-Charset:	ISO-8859-1,utf-8;q=0.7,*;q=0.7	
Keep-Alive:	300	
Connection:	keep-alive	
Cookie:	PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120	
Pragma:	no-cache	
Cache-Control:	no-cache	

HTTP headers as Name: Value

▶ 33

Cibercrime - Nuno Santos

2019



<http://amiunique.org>

Learn how identifiable you are on the Internet

Help us investigate the diversity of web browsers

[View my browser fingerprint](#)

By clicking on this button, only anonymous data will be collected and a cookie will be stored in your browser for four months. You can find more details in the [Privacy Policy](#).

Spread the word! Share AmIUnique!
Try it on all your devices!



▶ 34

Cibercrime - Nuno Santos

2019



Results on my browser

Are you unique?

Yes! (You can be tracked!)

35.80 % of observed browsers are Chrome, as yours.

2.66 % of observed browsers are Chrome 51.0, as yours.

13.82 % of observed browsers run Mac, as yours.

6.01 % of observed browsers run Mac 10.10, as yours.

66.20 % of observed browsers have set "en" as their primary language, as yours.

21.04 % of observed browsers have UTC+1 as their timezone, as yours.

However, your full fingerprint is unique among the 232283 collected so far. Want to know why? [Click here](#)

[View more details](#) [View graphs](#)

▶ 35 Cibercrime - Nuno Santos 2019



Perceber os detalhes desta identificação

Detail of the plugins		
Attribute	Similarity ratio ⓘ	Value
User agent ⓘ	<0.1%	"Mozilla/5.0 (Windows NT 10.0; Win10_10240) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2623.102 Safari/537.36"
Accept ⓘ	36.52%	"text/html, application/xhtml+xml, image/webp, */*
Content encoding ⓘ	7.36%	"gzip, deflate, br"
Content language ⓘ	<0.1%	"en-US, en;q=0.8"
List of plugins ⓘ	0.36%	"Plugin:OpenPGP; fgiehjal; iormat; inacn-plugin;r0; PepperCrypton; HTML adapter; p"

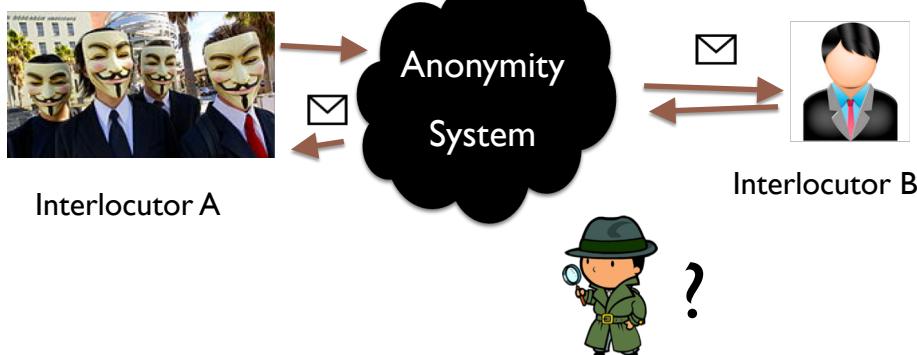
Detail of the browser		
Attribute	Similarity ratio ⓘ	Value
Platform	12.42%	"MacIntel"
Cookies enabled	78.34%	"yes"
Do Not Track ⓘ	49.71%	"NC"
Timezone	21.01%	"-60"
Screen resolution ⓘ	2.48%	"2560x1440x24"
Use of local storage ⓘ	74.73%	"yes"
Use of session storage ⓘ	74.73%	"yes"
Canvas	0.20%	"Cwm fjordbank glyphs next quiz, 😊"
WebGL Vendor ⓘ		"NVIDIA Corporation"
WebGL Renderer ⓘ		"NVIDIA GeForce GT 755M OpenGL Engine"
List of fonts ⓘ	15.90%	"Flash detected but not activated (click-to-play)"
Screen resolution ⓘ	15.90%	"Flash detected but not activated (click-to-play)"
Language ⓘ	15.90%	"Flash detected but not activated (click-to-play)"
Platform ⓘ	15.90%	"Flash detected but not activated (click-to-play)"
Use of Adblock ⓘ	45.16%	"no"

▶ 36 Cibercrime - Nuno Santos 2019



Anonymity systems

- ▶ Procuram ocultar a identidade dos interlocutores das comunicações



▶ 37

Cibercrime - Nuno Santos

2019



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

▶ 38

Cibercrime - Nuno Santos

2019



Quantificar o anonimato

- ▶ Como quantificar o quanto anónimos estamos?
 - ▶ Conjuntos de anonimato



- ▶ Quanto maior o conjunto = mais forte o anonimato

▶ 39

Cibercrime - Nuno Santos

2019



Exemplo em que não existe anonimato



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

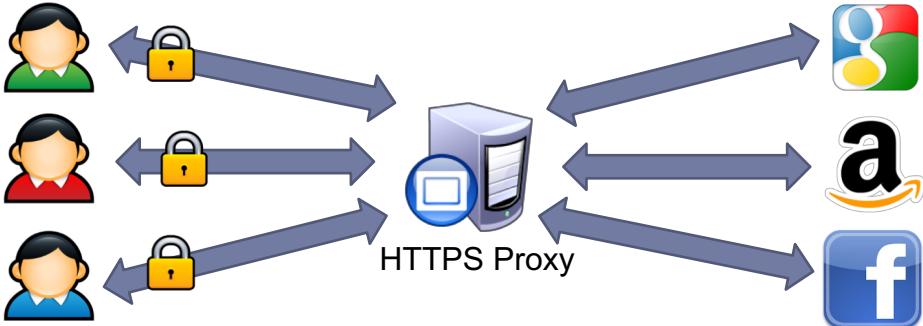
▶ 40

Cibercrime - Nuno Santos

2019



Abordagem básica: Proxies de anonimização

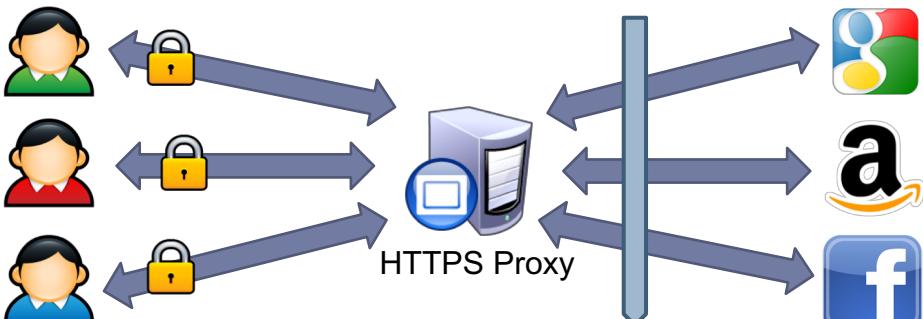


Web proxies reencaminham tráfego HTTPS traffic
ex., <https://www.anonymizer.com>, <http://www.bind2.com/>

▶ 41 Cibercrime - Nuno Santos 2019

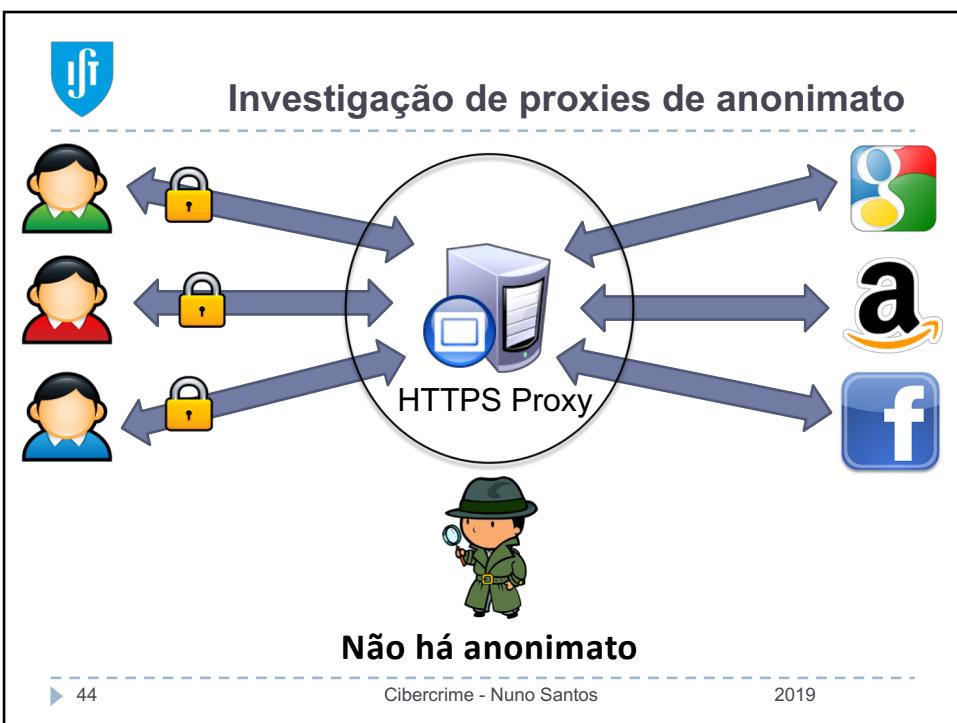
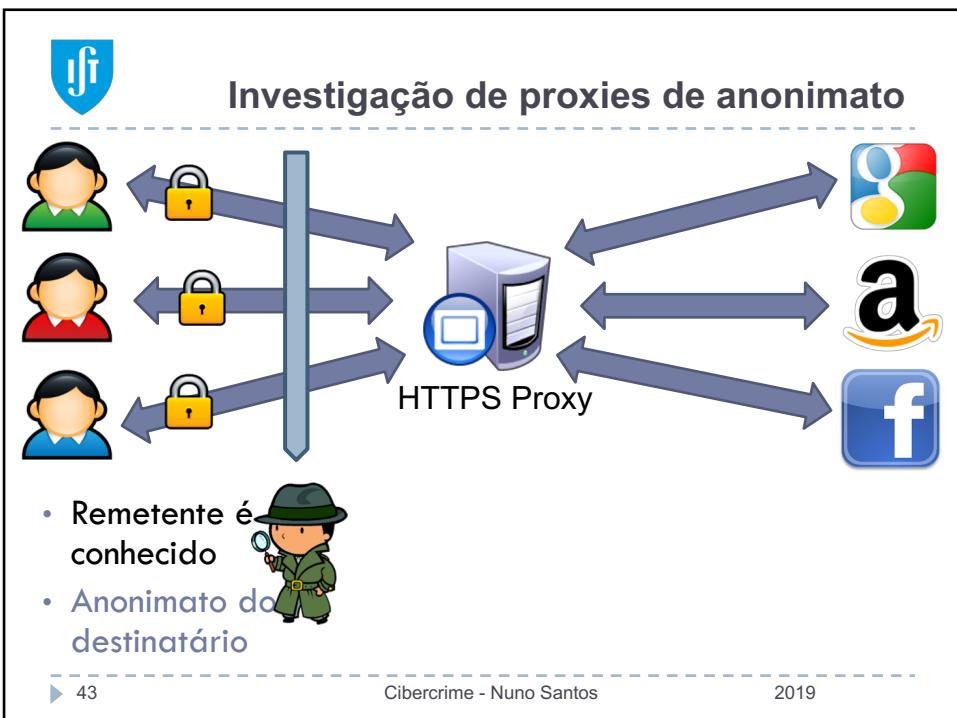


Investigação de proxies de anonimato

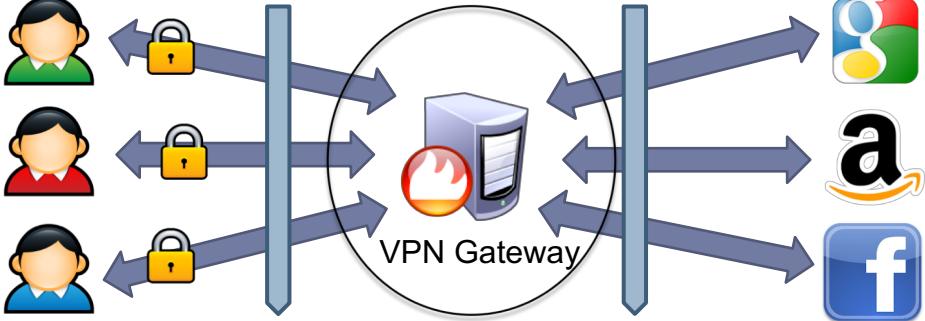


- O destino é conhecido
- Anonimato do remetente

▶ 42 Cibercrime - Nuno Santos 2019



 Mesmas propriedades para qualquer proxy



- Remetente é conhecido
- Anonimato do destinatário

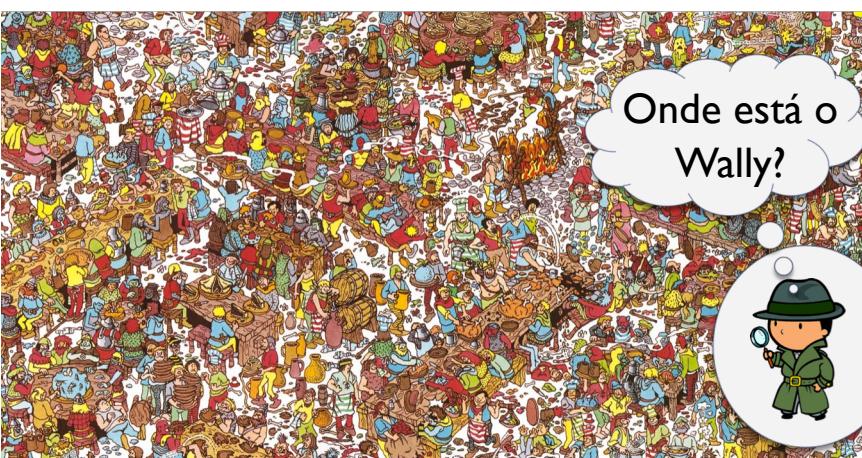
Não há anonimato

- O destino é conhecido
- Anonimato do remetente

▶ 45 Cibercrime - Nuno Santos 2019

 Aumentar protecção: Anonimato adora companhia

Mecanismo chave: misturar-se na multidão



▶ 46 Cibercrime - Nuno Santos 2019



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 populares: Tor, I2P
- ▶ Tor incorpora algumas ideias de **onion routing**

▶ 47

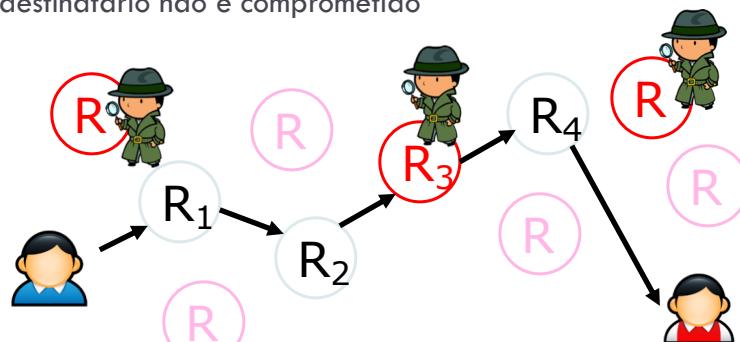
Cibercrime - Nuno Santos

2019



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



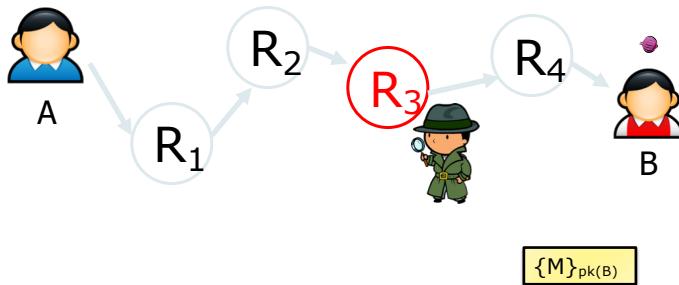
▶ 48

Cibercrime - Nuno Santos

2019



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

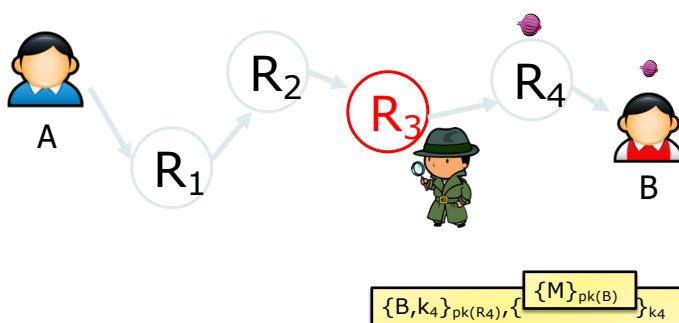
▶ 49

Cibercrime - Nuno Santos

2019



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

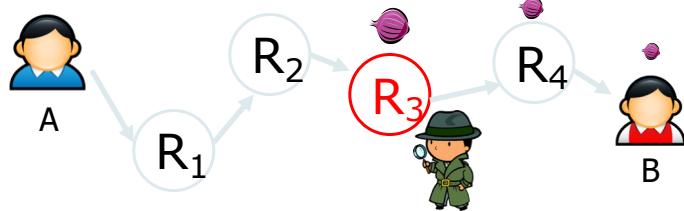
▶ 50

Cibercrime - Nuno Santos

2019



Route establishment in basic onion routing



$\{R_4, k_3\}_{pk(R_3)}, \{B, k_4\}_{pk(R_4)}, \{M\}_{pk(B)}$

$\{M\}_{pk(B)} k_4 k_3$

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

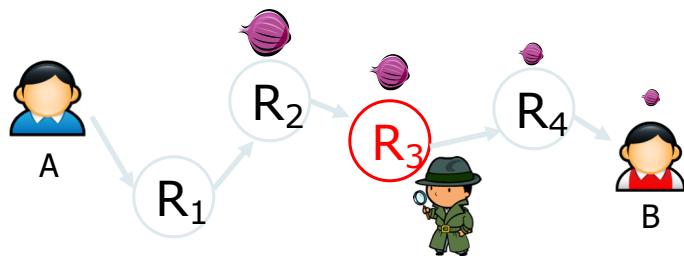
▶ 51

Cibercrime - Nuno Santos

2019



Route establishment in basic onion routing



$\{R_3, k_2\}_{pk(R_2)}, \{R_4, k_3\}_{pk(R_3)}, \{B, k_4\}_{pk(R_4)}, \{M\}_{pk(B)}$

$\{M\}_{pk(B)} k_3 k_2$

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

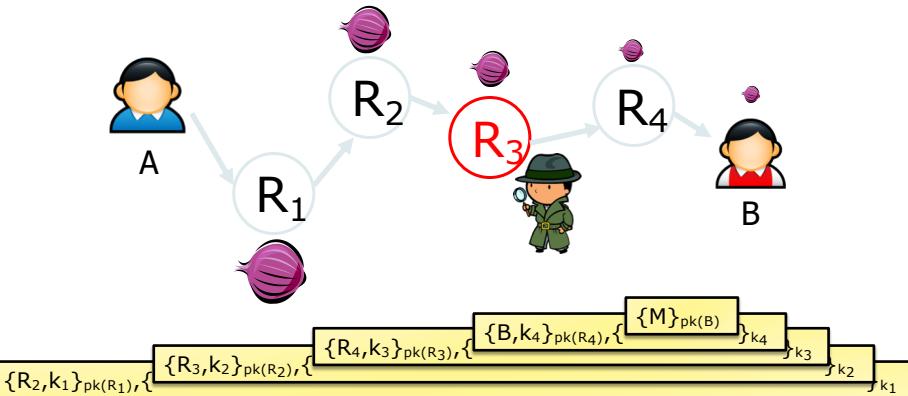
▶ 52

Cibercrime - Nuno Santos

2019



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

▶ 53

Cibercrime - Nuno Santos

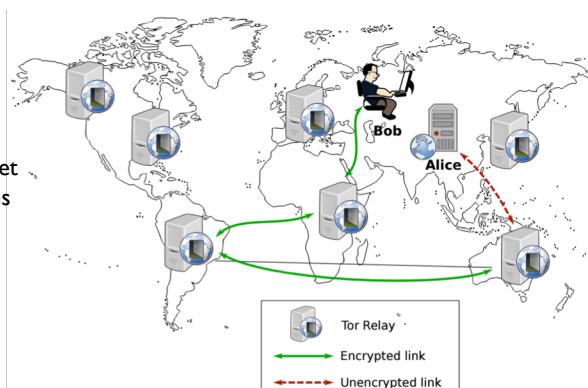
2019



Tor: A 2^a 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



▶ 54

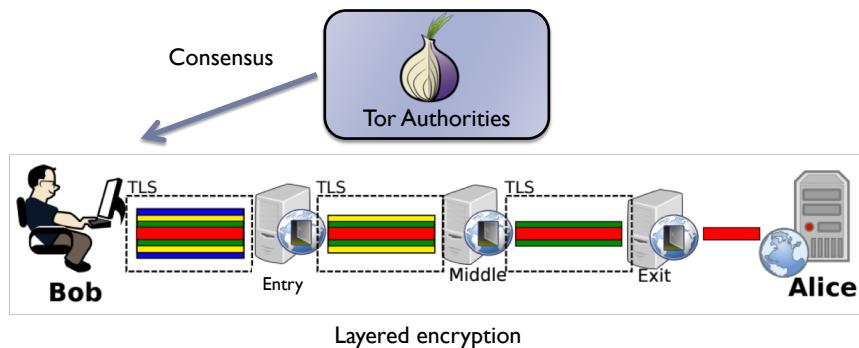
Cibercrime - Nuno Santos

2019



Tor circuit

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



▶ 55

Cibercrime - Nuno Santos

2019



Serviços ocultos

- ▶ Tor esconde o remetente, mas o destinatário é exposto
- ▶ E se o criminoso pretende ter um serviço web anônimo?
 - ▶ 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)

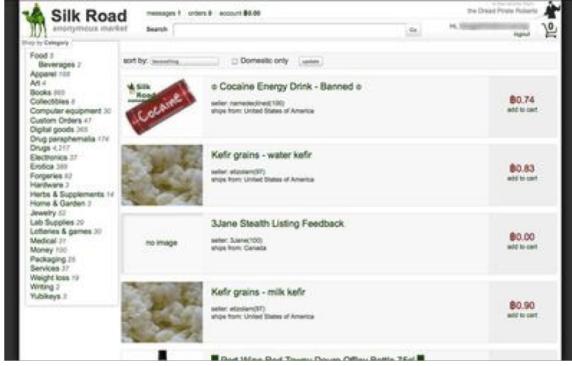
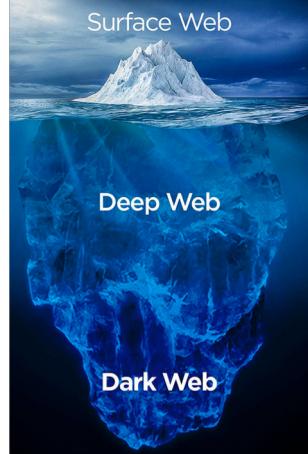


▶ 56

Cibercrime - Nuno Santos

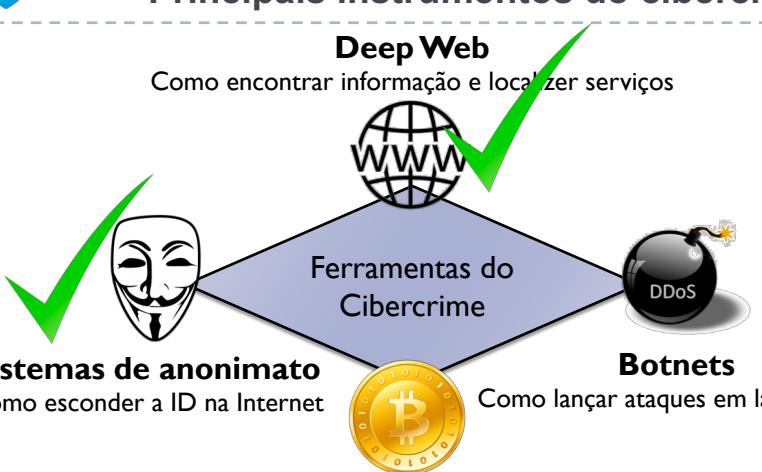
2019

Tor e serviços ocultos estão na base da Dark Web

▶ 57 Cibercrime - Nuno Santos 2019

Principais instrumentos do cibercrime



Deep Web
Como encontrar informação e localizar serviços

Sistemas de anonimato
Como esconder a ID na Internet

Criptomoeda
Como tornar os pagamentos não rastreáveis

Botnets
Como lançar ataques em larga escala

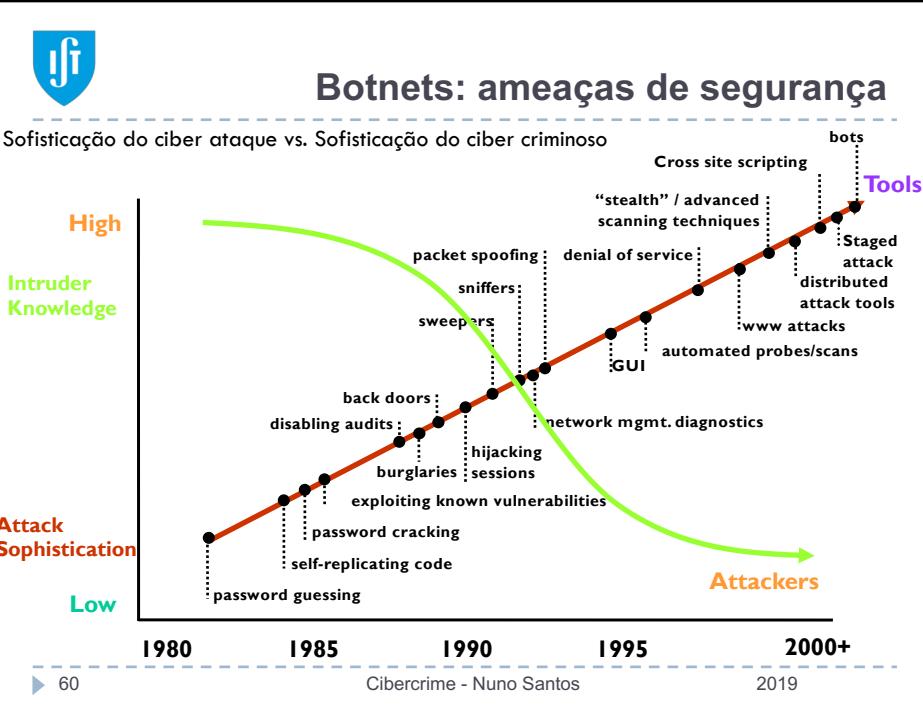
▶ 58 Cibercrime - Nuno Santos 2019

Botnets

59

Cibercrime - Nuno Santos

2019





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 infraestruturas e estados
- ▶ Um dos meios principais para actividade maliciosa

▶ 61

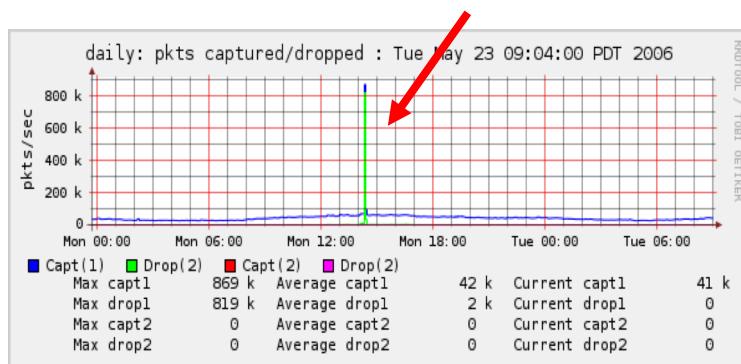
Cibercrime - Nuno Santos

2019



Ataques Distributed Denial-of-Service (DDoS)

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



▶ 63

Cibercrime - Nuno Santos

2019

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 Facebook: down and out again [along with Instagram] after DDoS attack? **27/01/2015**
By Darren Allan, CONTRIBUTING EDITOR

From the Twitter blog:

GitHub Status @githubstatus · Oct 22 We're investigating what appears to be a DDoS attack.

▶ 64 Cibercrime - Nuno Santos 2019

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

Attacker

Master machines

Zombie machines

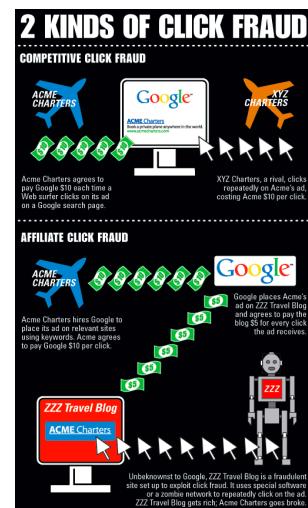
Victim

▶ 65 Cibercrime - Nuno Santos 2019



Botnet activities

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



▶ 66

Cibercrime - Nuno Santos

2019



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

▶ 67

Cibercrime - Nuno Santos

2019



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

▶ 68

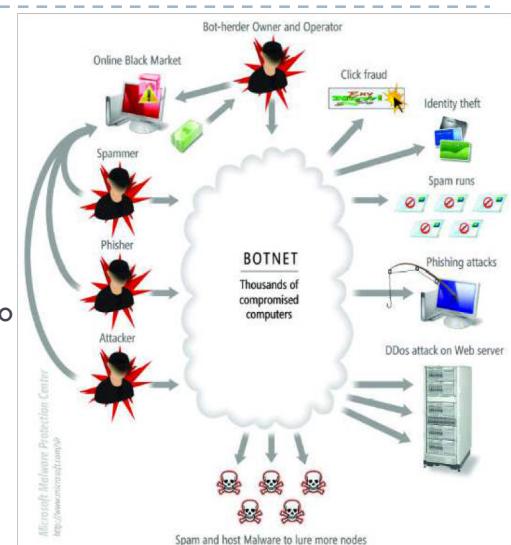
Cibercrime - Nuno Santos

2019



Botnet: Mercado global

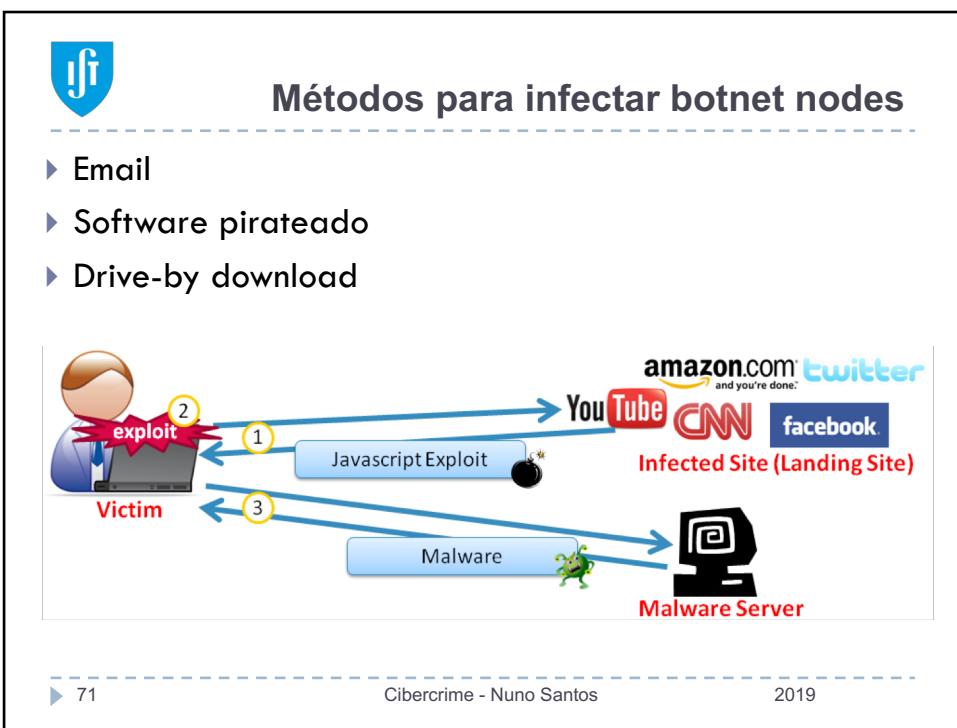
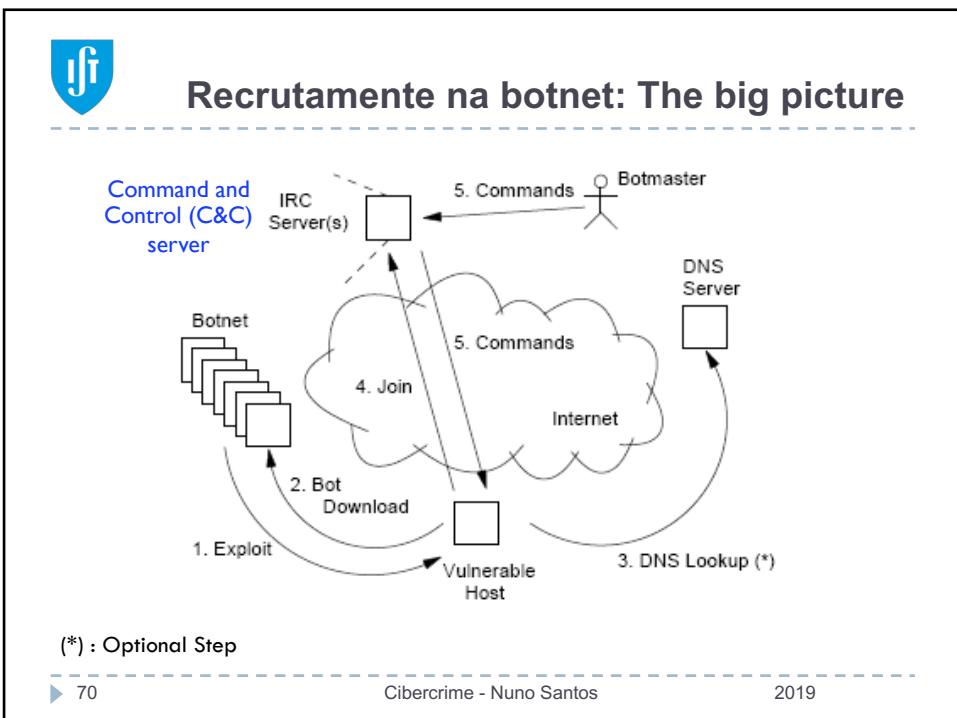
- ▶ Botmasters não são os únicos beneficiários
- ▶ Quem paga:
 - ▶ Internet Advertising companies for downloading adware onto vulnerable PCs
 - ▶ Companies who send spam, viruses and other malware
 - ▶ ...



▶ 69

Cibercrime - Nuno Santos

2019





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

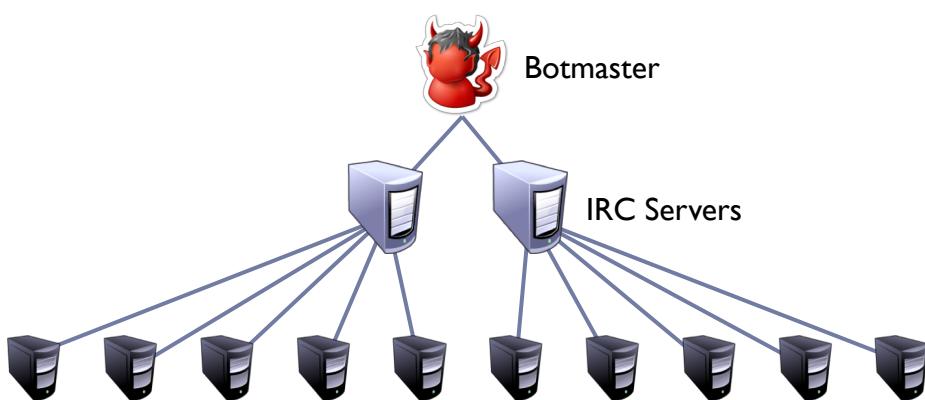
▶ 73

Cibercrime - Nuno Santos

2019



Arquitectura C&C centralizada



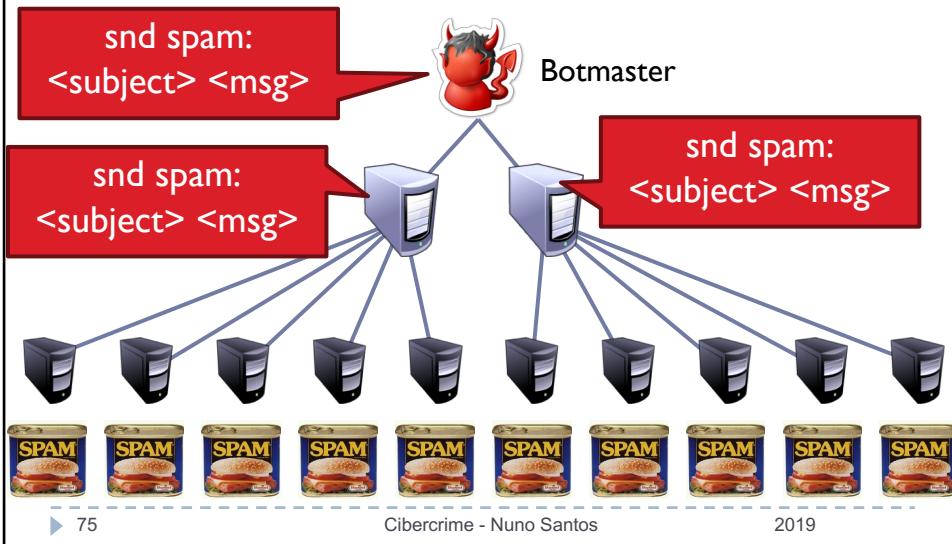
▶ 74

Cibercrime - Nuno Santos

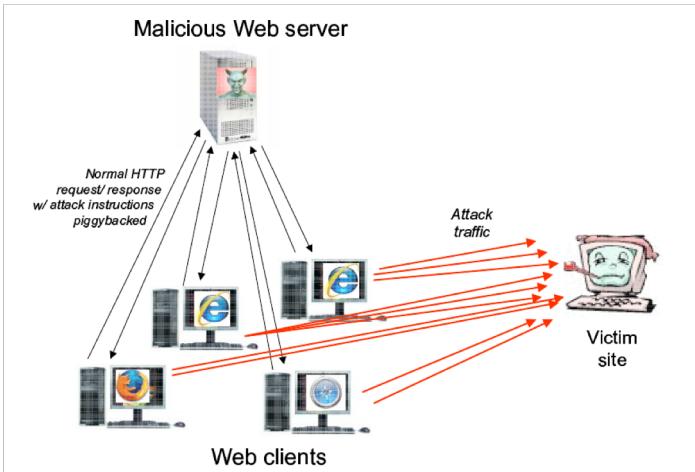
2019



Arquitectura C&C centralizada: Canais IRC



Usar HTTP



Serviços Web

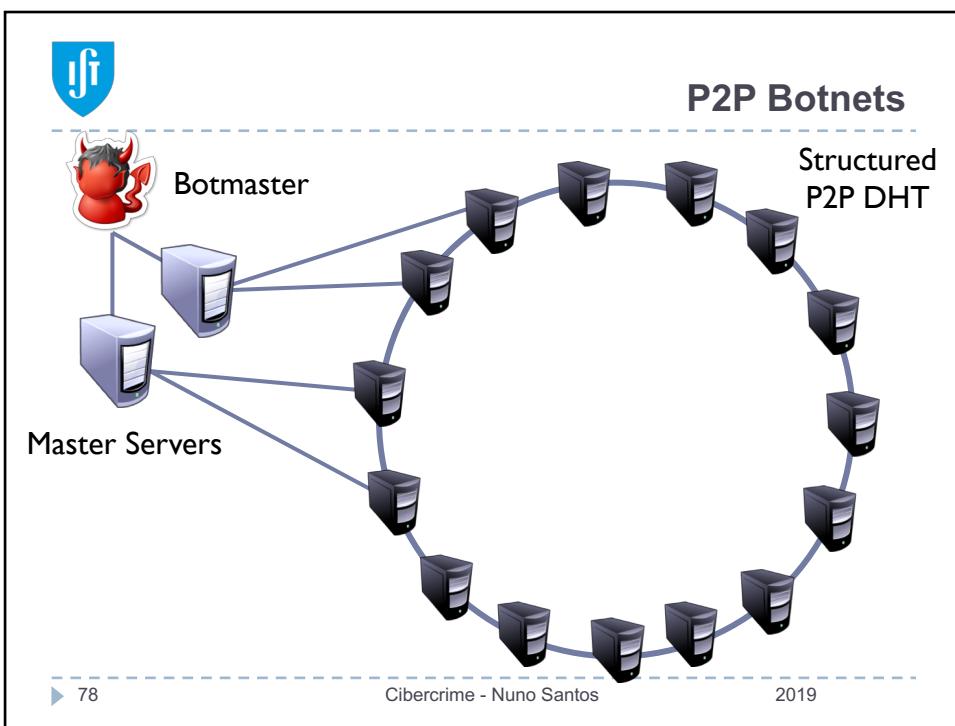
► Redes sociais começam a ser usadas para controlo de botnets

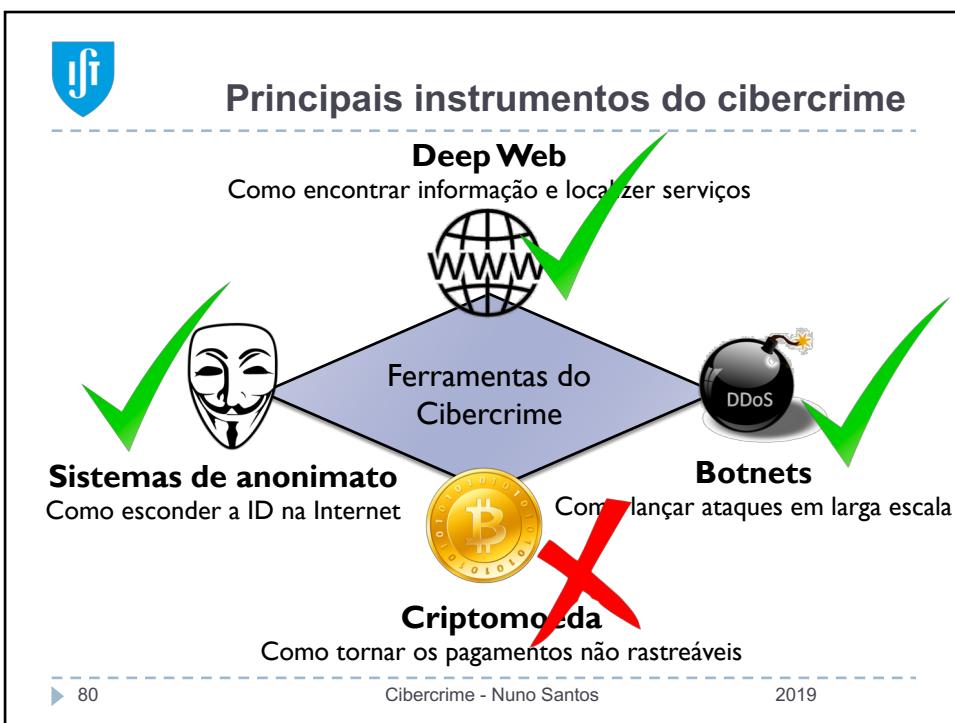
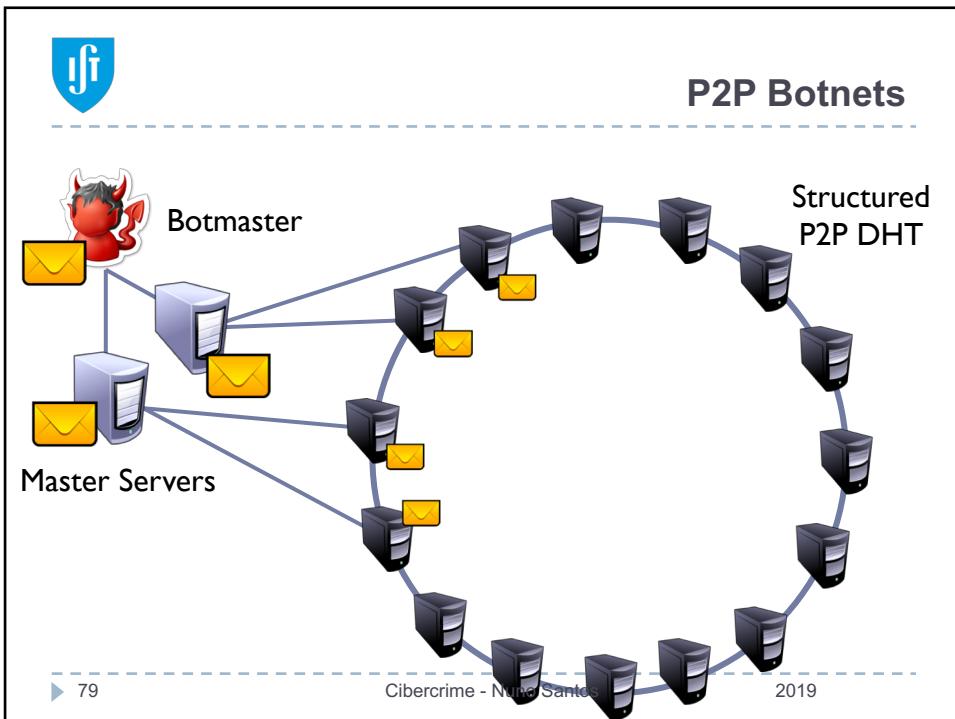


The screenshot shows a Twitter profile for a user named 'upd4t3'. The profile has 20 following and 7 followers. There are 25 tweets. The tweets contain various encoded strings, likely command-and-control (C2) messages used for botnet control.

► Botnets começam a atingir sistemas industriais e móveis

77 Cibercrime - Nuno Santos 2019







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

▶ 81

Cibercrime - Nuno Santos

2019



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 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

▶ 82

Cibercrime - Nuno Santos

2019



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