



**INTERCEPT**

Cyber intelligence

# The Web, The Deep Web & The Dark Web



**INTERCEPT** WATCH OUT BE PREPARED  
Cyber intelligence

# In The Beginning There Was The Internet

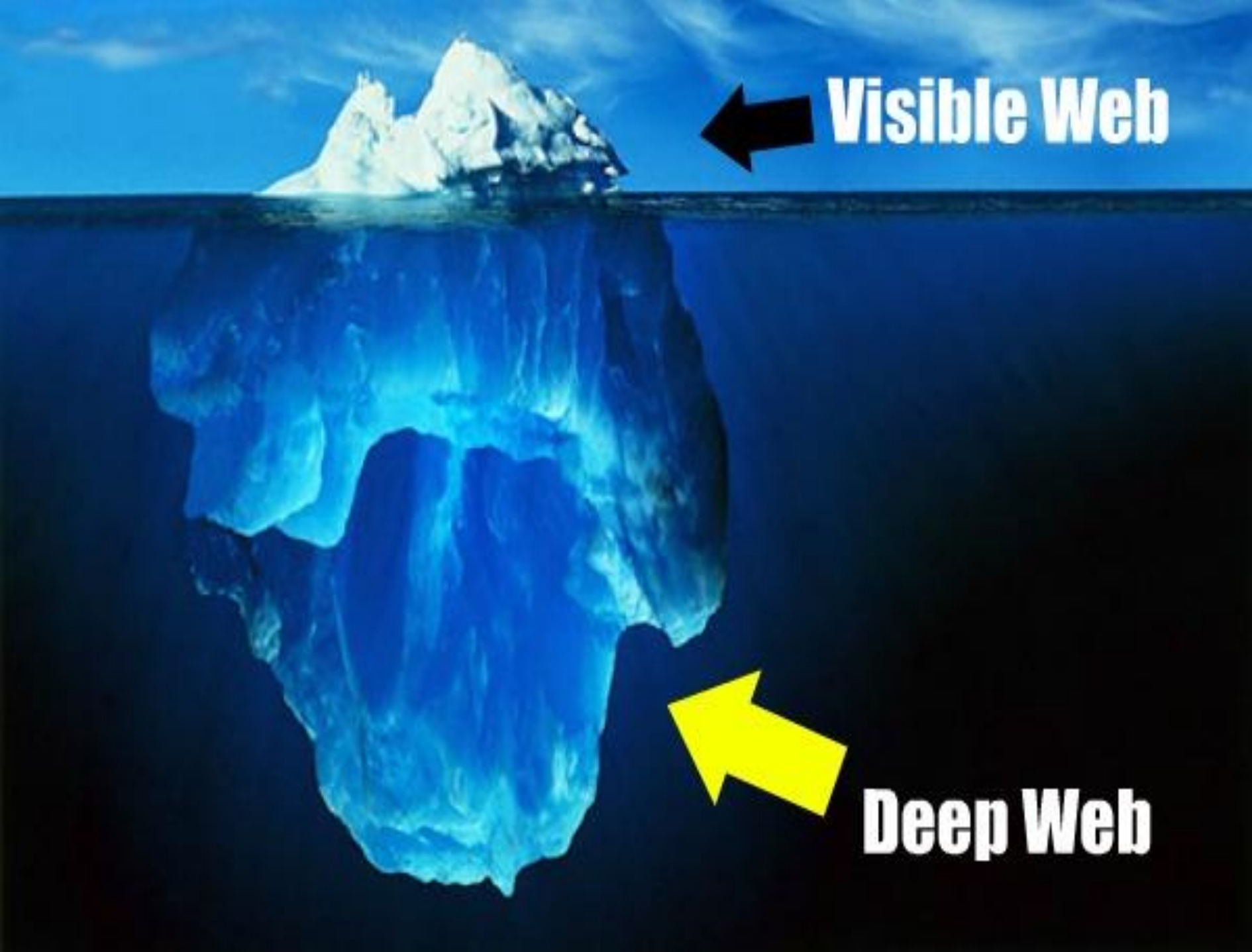




You are here

# The World Wide Web

Search engines and especially Google have revolutionized the field of informatics and created a new field of intelligence – WEBINT.



**Visible Web**

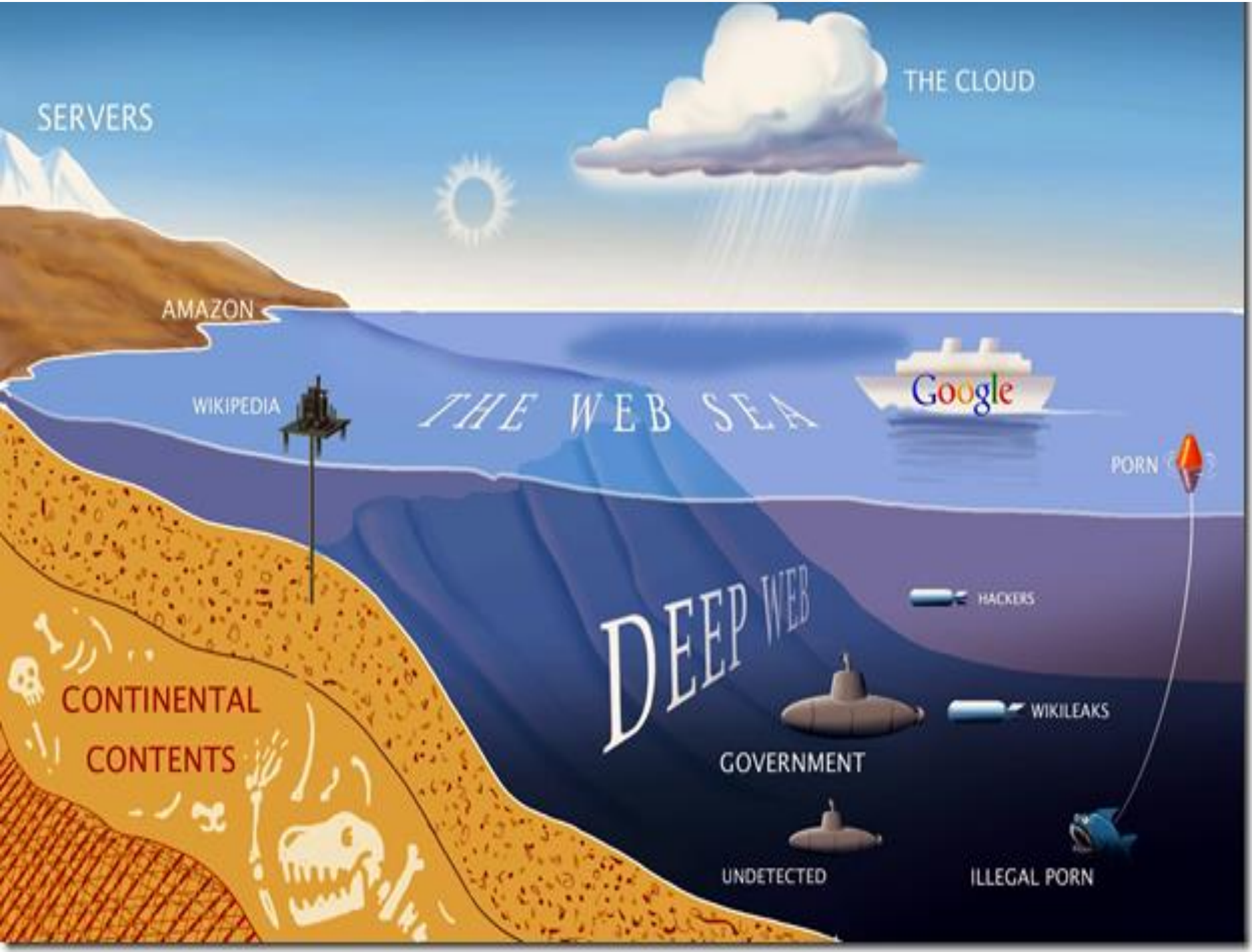


**Deep Web**



# The Deep Web

The Deep Web includes all online information that cannot be harvested by Google



SERVERS

THE CLOUD

AMAZON

WIKIPEDIA

THE WEB SEA

Google

PORN

DEEP WEB

HACKERS

WIKILEAKS

GOVERNMENT

UNDETECTED

ILLEGAL PORN

CONTINENTAL CONTENTS



# TOR – The Dark Web

- TOR is a network that enables anonymity and encryption while transferring information.
- TOR created the Dark Web which is the cyber under world.

# Online Crimes


- Hacking
- Hacktivists
- Data theft
- Espionage
- Online financial crimes
- Forbidden publications or trade.

# Terrorist Acticity

## Propaganda

جهاد | Jihad | speck

"We have the ability to make and use chemicals and poisonous gas. And those gases and poisons are made of the simplest ingredients, which are available in the pharmacies and we could, as well needed. And this is for use against vital institutions and residential areas."



### The Al Qaeda Manual

The attached manual was located by the Manchester (England) Metropolitan Police during a search of an al Qaeda member's home. The manual was found in a computer file described as "the military series" related to the "Declaration of Jihad." The manual was translated into English and was introduced earlier this year at the embassy bombing trial in New York.

### How can I Train Myself for Jihad

#### Disclaimer

#### 1.0 What is Jihad

#### 2.0 Military Training is an Islamic Obligation not an Option

#### 3.0 Sincerity of Intention

#### 4.0 Training in your Country of Residence

#### 4.1 Physical Training

#### 4.2 Martial Arts

#### 4.3 Survival and Outdoors Training

#### 4.4 Firearms Training

#### 4.5 Important Note on Live-Ammunition Jihad Firearms Training within the UK

#### 4.6 Military Training

#### 5.0 Jihad Training Abroad

"And prepare against them all you can of power, including steeds of war to terrorise the enemies of Allah and others besides whom you may not know, but Allah does know. And whatever you shall spend in the Cause of Allah shall be repaid unto you, and you shall not be treated unjustly." [Quran 8:60]

In commenting on this verse, the Messenger (SAWS) said:

"Indeed, power is shooting, power is shooting." [Sahih Muslim]

Narrated Abu Hurairah (RA) that the Messenger (SAWS) said:

"If anyone keeps a horse for Jihad in the Way of Allah, motivated by his faith in Allah and his belief in His Promise, then he will be rewarded on the Day of Resurrection for what the horse has eaten or drunk and for its dung and urine." [Sahih Al-Bukhari]

After receiving a number of e-mails asking about this topic, we decided to include a small article about this subject. It is broken down into sections, but should be read from beginning to end for maximum benefit.

HOUSE

zing the Middle East and

Jihad [Holy War] Against

ompassionate

day and night...  
ngs these phrases...  
ing for with the apostate  
., Platonic ideals...  
the dialogue of  
mbing, and destruction,  
ine-gun.

never be established  
ve councils. They are

# Hacking

**Rent-A-Hacker** [Products](#) [FAQs](#) [Register](#) [Login](#)

## Rent-A-Hacker

**Experienced hacker offering his services!**

(Illegal) Hacking and social engineering is my business since i was 16 years old, never had a real job so i had the time to get really good at hacking and i made a good amount of money last +-20 years.  
I have worked for other people before, now im also offering my services for everyone with enough cash here.

**Prices:**  
Im not doing this to make a few bucks here and there, im not from some crappy eastern europe country and happy to scam people for 50 euro.  
Im a professional computer expert who could earn 50-100 euro an hour with a legal job.  
So stop reading if you dont have a serious problem worth spending some cash at.  
Prices depend alot on the problem you want me to solve, but minimum amount for smaller jobs is 200 euro.  
You can pay me anonymously using Bitcoin.

**Technical skills:**

- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successfull, if i dont know it, ill learn it very fast
- Anonymity: noone will ever find out who i am.

**Social Engineering skills:**

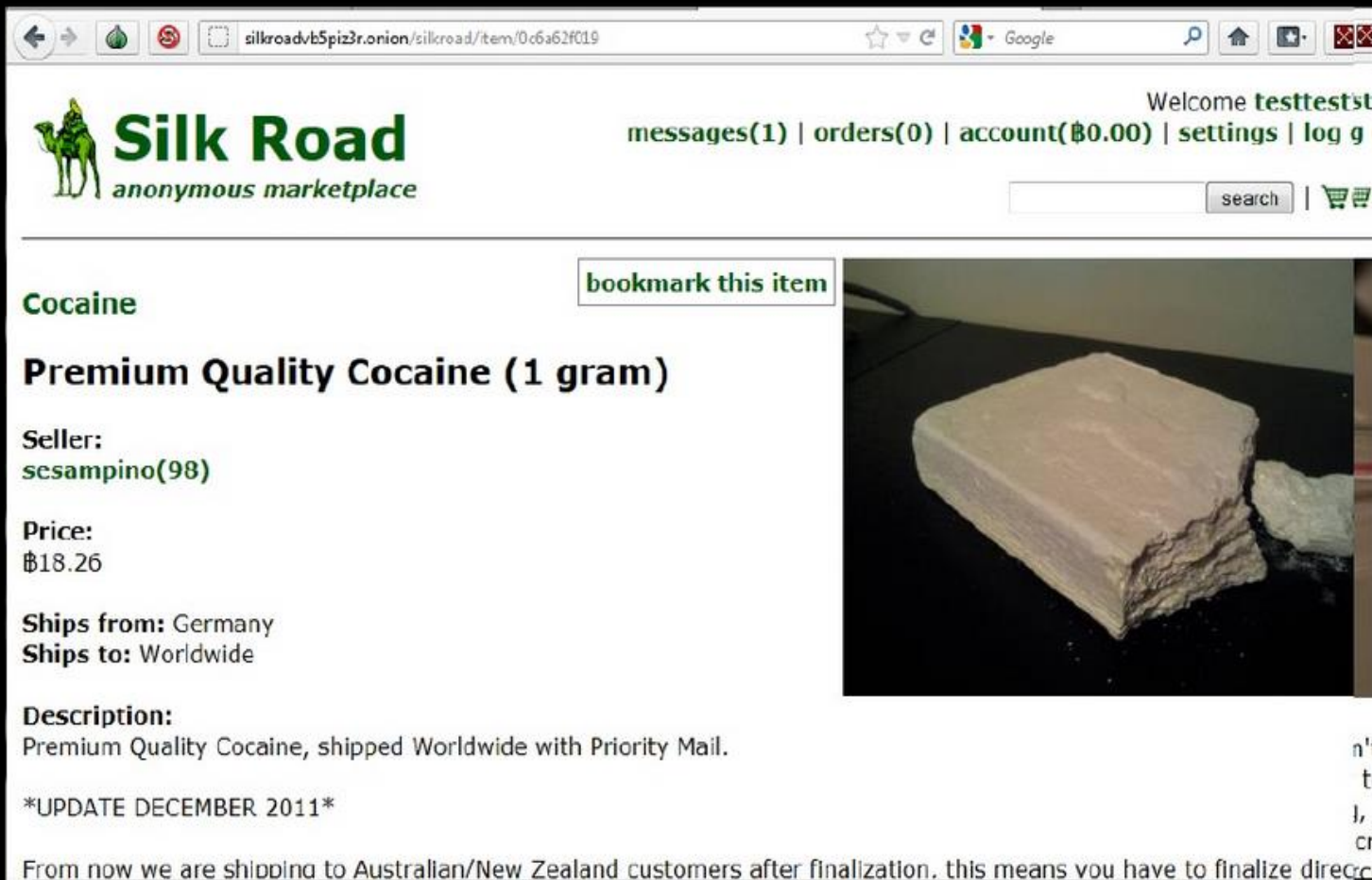
- Very good written and spoken (phone calls) english and german.
- If i cant hack something technically ill make phone calls or write emails to the target to get the needed information, i have

# Stolen Files and Info

Name	Date	Time	Filesize
<a href="#">0dayfrsec</a>	01/21/2014	18:55:17	4.97 KB
<a href="#">1ASI0w</a>	01/02/2014	00:08:01	0.27 KB
<a href="#">1Chris</a>	11/02/2013	20:50:09	0.38 KB
<a href="#">1Fast</a>	08/23/2013	00:04:29	0.89 KB
<a href="#">1fresh_name_ss_dob</a> This file contains an SSN.	12/23/2013	05:37:36	0.67 KB
<a href="#">2Fast 2fast4race basscode</a>	05/12/2013	10:59:51	0.88 KB
<a href="#">2moto the FBI informat</a> This file contains entries from hacked databases.	11/27/2013	02:03:40	2.95 KB
<a href="#">2 Chainz</a> This file contains an SSN.	10/09/2013	17:49:16	1.03 KB
<a href="#">3rd Eye RC</a>	06/28/2013	18:14:14	0.4 KB
<a href="#">5h4d0w SynthGlow</a>	09/10/2013	05:49:31	0.34 KB
<a href="#">6Scroll</a>	03/27/2013	00:12:39	0.09 KB
<a href="#">11AmericanFunFest</a> This file contains SSNs.	09/03/2013	05:14:23	5.48 KB
<a href="#">35k Israelis Part 1</a>	11/17/2012	03:44:01	686.38 KB
<a href="#">35k Israelis Part 2</a>	11/17/2012	03:44:06	670.43 KB
<a href="#">35k Israelis Part 3</a>	11/17/2012	03:44:13	631.51 KB
<a href="#">35k Israelis Part 4</a>	11/17/2012	03:44:22	634.16 KB
<a href="#">35k Israelis Part 5</a> This file contains mail. This file contains entries from leaked databases	01/04/2014	01:02:10	656.16 KB

# Drug Commerce

## Silk Road



The screenshot shows a web browser window displaying the Silk Road marketplace. The browser's address bar shows the URL `silkroadvb5piz3r.onion/silkroad/item/0c6a62fc19`. The page header includes the Silk Road logo (a green camel) and the text "Silk Road anonymous marketplace". Navigation links include "Welcome testtest", "messages(1)", "orders(0)", "account(฿0.00)", "settings", and "log g". A search bar and a shopping cart icon are also visible.

**Cocaine** [bookmark this item](#)

**Premium Quality Cocaine (1 gram)**

**Seller:**  
sesampino(98)


**Price:**  
฿18.26

**Ships from:** Germany  
**Ships to:** Worldwide

**Description:**  
Premium Quality Cocaine, shipped Worldwide with Priority Mail.

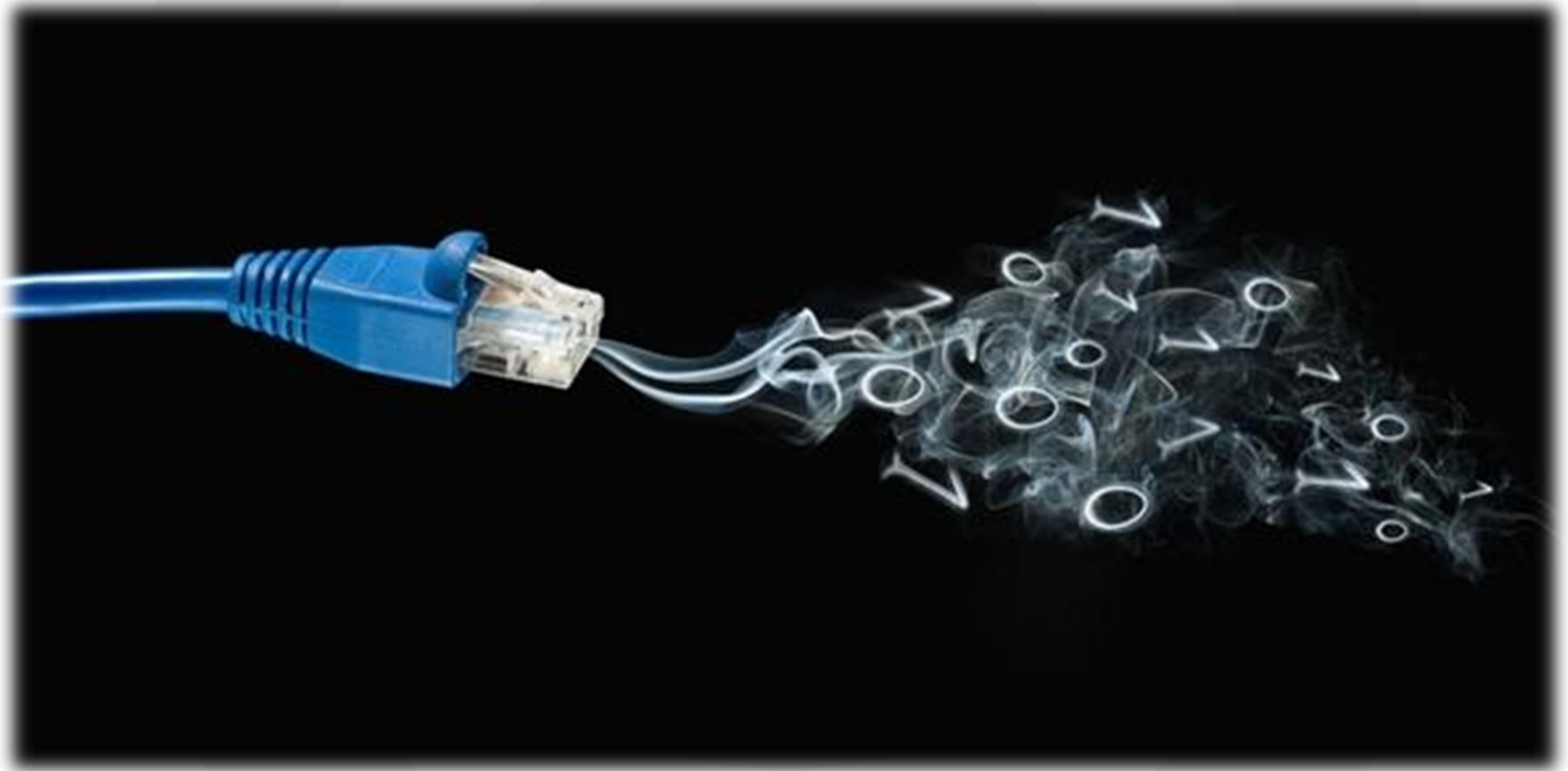
\*UPDATE DECEMBER 2011\*

From now we are shipping to Australian/New Zealand customers after finalization. this means you have to finalize direc



# Commercial Threats

# Leakage Alert Service





# Preliminary Leakage

```
reddish applo@hotmail.com| heyhey  
kate@krcreative.com.au| millard  
gotchavanessa@bigpond.com| porthcurno
```

```
899. "Superyacht - Contacts", "jcarneuk@yahoo.co.uk", "None", "776", "None", "0"  
900. "Superyacht - Contacts", "master@my-sputnik.com", "Jason", "777", "Farr", "0"  
901. "Superyacht - Contacts", "rabdan.captain@alseermarine.ae", "Chris", "778", "Lewis", "0"  
902. "Superyacht - Contacts", "captain@yacht-pegasus.com", "Martyn", "779", "Walker", "0"  
903. "Superyacht - Contacts", "master@ultimaiii.com", "Owen", "780", "Jones", "0"  
904. "Superyacht - Contacts", "master@myqueenk.com", "Peter", "781", "Read", "0"  
905. "Superyacht - Contacts", "fabien@felicitaewest.com", "Fabien", "782", "Roche", "0"  
906. "Superyacht - Contacts", "captain@my-aviva.com", "Charles", "783", "Hacker", "0"  
907. "Superyacht - Contacts", "s-y-atmosphere@attglobal.net", "Neil Batt", "784", "None", "0"  
908. "Superyacht - Contacts", "peter.chisholm@pccmc.net", "Peter", "785", "Chisholm", "0"  
909. "Superyacht - Contacts", "captain@mylittleviolet.com", "Adrian", "786", "Croft", "0"  
910. "Superyacht - Contacts", "captain@myladychristina.com", "None", "787", "None", "0"  
911. "Superyacht - Contacts", "richard@mqiv.com", "Richard", "788", "Kirkbly", "0"  
912. "Superyacht - Contacts", "captain@my-anna.com", "Paul", "789", "Cook", "0"
```

```
kat1508@hotmail.com| ll226w  
kate409@hotmail.com| pac112  
fiona@popmedia.info| fifistack
```

# Significant Leakage

Reference ID	Created	Released	Classification	Origin
05PARIS1142	2005-02-23 12:12	2011-02-10 08:08	CONFIDENTIAL	Embassy Paris
<p>Appears in these articles: <a href="http://abonnes.lemonde.fr/documents-wikileaks/article/2011/02/09/wikileaks-les-visiteurs-de-l-ambassade_1477418_1446239.htm">http://abonnes.lemonde.fr/documents-wikileaks/article/2011/02/09/wikileaks-les-visiteurs-de-l-ambassade_1477418_1446239.htm</a></p>				
<p>This record is a partial extract of the original cable. The full text of the original cable is not available.</p>				
<p>C O N F I D E N T I A L SECTION 01 OF 02 PARIS 001142</p> <p>SIPDIS</p> <p>STATE FOR EUR/WE, EUR/ERA, EB/TPP STATE PASS TO USTR (VERONEAU, NOVELLI, SANFORD) COMMERCE FOR GRANT ALDONAS AND FRED ELLIOTT</p> <p>E.O. 12958: DECL: 02/22/2015 TAGS: ETRD EAIR SCUL FR WTR0 USTR SUBJECT: ARNAUD LAGARDERE ON BOEING/AIRBUS, CHIRAC AND THE MEDIA</p> <p>REF: A. 04 PARIS 9014 B. PARIS 372</p> <p>Classified By: Econ Minister-Counselor Thomas J. White for reasons 1.5 (b) and (d).</p>				

# Credentials Leakage

## RAW Paste Data

```
jongs.3unubot@gmail.com,10130  
jongbong@tta.or.kr,ttajongbong  
jorgen.friis@etsi.org,jfretsi  
jsmith@numerex.com,brocklee  
k-kenyoshi@cb.jp.nec.com,kindjpyut  
ka-matsuo@kddi.com,matsuo7722  
kagami.osamu@lab.ntt.co.jp,akira000  
karen.higginbottom@hp.com,none  
kdj@tta.or.kr,ttakdj  
kentb@qualcomm.com,perhaps  
khj@etri.re.kr,helios21
```

# Scripts Leakage

```
38. /**
39.  * swiftトピックのメッセージを受信し標準出力するRunnableタスク
40.  * enemanetトピック用のconsumer
41.  *
42.  * @author NTT DATA
43.  *
44.  */
45. public class Consumer implements Runnable {
46.
47.     private final String JDBC_DRIVER = "com.mysql.jdbc.Driver";
48.     private String dbName = "mydb";
49.     private String dbUserName = "root";
50.     private String dbPassword = "123456789";
51.     private String connectionString = "jdbc:mysql://192.168.0.18/" + dbName + "?user=" + dbUserName + "&password=" + dbPassword +
"&useUnicode=true&characterEncoding=UTF-8";
52.
53.     // Database credentials
54.     private final String USER = "root";
55.     private final String PASS = "123456789";
56.
57.     private static final Logger logger = Logger.getLogger(Consumer.class);
58.     private KafkaStream stream;
59.     private SwiftConfig swiftConfig;
60.     private SimpleDateFormat sdf;
```

# Info about IT Infrastructure

```
0.0.0.0 stags.peer39.net #[PrivacyChoice.Tracker]
# [Ntt America][198.104.0.0 - 198.104.255.255]
0.0.0.0 www.secure-processingcenter.com
0.0.0.0 www.spywarebegone.com
0.0.0.0 www.zipitfast.com
# [Ntt America][198.63.0.0 - 198.66.255.255]
0.0.0.0 ads.drugs.com
0.0.0.0 ads.egloomedia.com
0.0.0.0 www.spyarsenal.com #[Spyware.DesktopSpy][Spyware.FamilyKeyLog]
# [Ntt America][199.236.0.0 - 199.239.255.255]
0.0.0.0 www.tsgonline.com
# [Ntt America][199.4.64.0 - 199.4.127.255]
```

# Hackers Discussions

```
24. Banks supporting stock exchange:
25.
26. www.fpb.com.mm
27.
28. www.mcb.com.mm
29.
30. http://tunfoundationbankmyanmar.com
31.
32. http://yomabank.com.mm
33.
34. http://www.kzbank.com
35.
36. http://cbbank.com.mm/
37.
38. http://treasurebankmm.com
39.
40. http://mobbankmm.com
41.
42. http://ayabank.com
43.
```

```
1. Target:
2. Myanmar (Burma)
3. Ministry of Immigration &
4. http://www.dop.gov.mm
5.
6. Nmap scan report for 203.1
7. Host is up (0.57s latency).
8. Not shown: 994 filtered ports
9. PORT      STATE SERVICE      VERSION
10. 80/tcp    open  http         Apache httpd 2.4.12 ((Win32) OpenSSL/1.0.11 PHP/5.6.8)
11. | http-cookie-flags:
12. |   /:
13. |   PHPSESSID:
14. |   httponly flag not set
15. |_http-server-header: Apache/2.4.12 (Win32) OpenSSL/1.0.11 PHP/5.6.8
16. | http-title: Ministry of Immigration & Population
17. | Requested resource was http://203.81.89.239/moip/
```

```
Target : -
http://www.mofa.gov.mm/
www.ncgub.net/
http://www.erepublic.org/egovincountriesmoni/myanmarformerlyburma.html
http://www.myanmar.com/ministries/index.html
```

```
[ : Denial-of-service attack & Deface Programs : ]
http://www.mediafire.com/?3j9lp4avc1tjplt
```

```
[ : Cyber Ghost VPN Program : ]
http://cyberghostvpn.com/
```

```
[ : Free Emails To Use VPN : ]
http://pastebin.com/G9yQhHmg
```

```
28. [ : First Myanmar Website Target : ]
29. www.dmh.gov.mm/ 203.81.81.131
30. Ports / 80 / 443 - FIRE!!
31.
32. .gov.mm websites /
33. http://www.dca.gov.mm/
34. http://www.myanmarevisa.gov.mm/
35. http://www.mot.gov.mm/
36. http://www.iwt.gov.mm/
37. http://www.nlm.gov.mm/
38. http://www.4thgmssummit.gov.mm/
39. http://www.dmh.gov.mm/
40. http://www.mofa.gov.mm/
```

**So to find the important  
information you must scan the  
surface web, the deep web and  
the dark web**

# Searching The Dark Web

- Most of the dark web is unindexed, and therefore we will not find its contents in Google.
- Unstable sites – closed or shifting URLs.
- Password protected sites.
- Viruses hazards.



# Cyber Spies (Avatars)

We participate in closed forums, thus learn about threat actors' intentions, plans, teams, execution, methods, etc.



# Questions?



**INTERCEPT** WATCH OUT BE PREPARED  
Cyber intelligence