The logo for DataSploit features the text "DataSploit" in a large, black, sans-serif font. The letter "Q" is stylized as a magnifying glass. A black line with five circular nodes is overlaid on the text, starting from the bottom left, passing through the "p", "l", and "o", and ending at the top right of the "Q".

# DataSploit

Open Source Assistant for #OSINT

<https://github.com/datasploit/datasploit>

<http://datasploit.info> | @datasploit

```
[shubhammittal:// $ whoami
```

- Just another Pen-tester.
- Security Consultant @ NotSoSecure
- 5+ Years of Experience
  
- Twitter - @upgoingstar
- Email - upgoingstar@gmail.com

# What's DataSploit?

- Automated OSINT Tool for Domain / Email / Username / IP Addresses
  - Fetches information from multiple HIDDEN sources.
  - Works in passive mode.
  - Written in Python.
  - Multiple report formats available.
- 
- Customized for Pen-testers / Product Security Guys / Cyber Investigators.

# Why DataSploit?

- So much data.
  - Server's Username / Passwords
  - Address
  - Email Id
  - Phone Number
  - Credentials
  - Interests
  - Friends
  - Preferences
  - Legacy Machines
  - Unnecessary Ports Information
  - Technologies in use, and blah blah..

# Lets talk real time? History?

Well, you see it coming. What I found within 30 minutes was really stunning:

- 6 AWS access keys with their secret tokens
- 3 MongoDB connection URI (with login and password)
- 1 Twitter API credentials
- 1 Twilio API credentials
- 1 GitHub account credentials
- 1 Gmail account credentials
- And 1 Ravello Systems account credentials

## Removed credentials

master

Browse files

committed 9 days ago

1 parent

commit

Showing 1 changed file with 5 additions and 5 deletions.

Unified Split

group\_vars/all

View

```
1 1 # Ravello's Credentials
2 -username: [REDACTED]@redhat.com
3 -password: [REDACTED]
4 -bucket: [REDACTED]
5
6 +#username:
7 +#password:
8 +#bucket:
```

June 25, 2015

Study: Leaked credentials on Pastebin.com linked to 47 gov't agencies



credentials leaked site:pastebin.com



All

Images

News

Videos

Maps

More

Settings

Tools

About 1,140 results (0.40 seconds)

## Leaked Steam Credentials <3 - Pastebin.com

[pastebin.com/cDQX04AQ](https://pastebin.com/cDQX04AQ)

Leaked Steam Credentials <3. a guest Jul 3rd, 2015 262 Never. Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

## Philippine Information Agency Full Credentials Leaked - Pastebin.com

[pastebin.com/TWuKVS95](https://pastebin.com/TWuKVS95)

Dec 28, 2013 - Philippine Information Agency Complete User Credentials Leaked. Website: http://news.pia.gov.ph. Country: Philippines. Database: pianews.

## FULL INSTAGRAM DATABASE LEAKED 2017 - Pastebin.com

[pastebin.com/R6VfmHrJ](https://pastebin.com/R6VfmHrJ)

Jan 27, 2017 - Whether or not the leaked Instagram credentials are authentic, it never hurts to change ... Searches related to Instagram database leak ...

## 25+ Leaked TWC Account Login Credentials - \*\*NEW MAY 2016 ...

[pastebin.com/5tiyxT3E](https://pastebin.com/5tiyxT3E)

25+ Leaked TWC Account Login Credentials - \*\*NEW MAY 2016\*\*. a guest May 25th, 2016 284 Never ... Leaked by: xjkn3rX. Full Dump: COMMENCED ...

## Leaked User Credentials of Nice Print Photography & PIAP PH ...

[pastebin.com/gy8HsgHE](https://pastebin.com/gy8HsgHE)

Leaked User Credentials of Nice Print Photography & PIAP PH. a guest Oct 11th, 2015 1,230 Never. Not a member of Pastebin yet? Sign Up, it unlocks many ...

TWITTER LEAKED DATABASE NEW ...

# Components

- Domain Osint
- Email Osint
- IP Osint
- Username Osint
  
- WIP
  - Company Scoping
  - Phone Number OSINT
  - Active Modules

# Sources and Flow

## Domain:

WhoIS  
DNS Records  
PunkSpider  
Wappalyzer  
Github  
Email Harvester  
Domain IP History  
Paste(s) Search  
Pagelinks  
Wikileaks  
Links from Forums  
Passive SSL Scan  
ZoomEye  
Shodan  
Censys  
Subdomains



## Email:

Basic Email Checks  
Work History  
Social profiles  
Enumerated Usernames  
Location Information  
Slides  
Scribd Documents  
Related Websites  
HaveIBeenPwned



## Username:

Git Details  
Check username on various sites.  
Profile Pics –Output saved in  
\$username directory  
Frequent Hashtags  
Interaction on Twitter.

Active Modules

# Setting it up..

- Manual

- Download from git (git clone or download)  
git clone <https://github.com/DataSploit/datasploit.git>
- pip install -r requirements.txt
- config.py holds API keys
- **domain\_xyz.py** – running stand alone scripts.
- **domainOsint / emailOsint / ipOsint** – automated OSINT
- active\_scan.py

- Automated

- <https://hub.docker.com/r/appsecco/datasploit/>
- <https://hub.docker.com/r/ftorn/datasploit/>



# Documentation.

<https://datasplit.github.io/datasplit/>

https://datasplit.github.io/datasplit/apiGeneration/

How to Generate Api Keys

Search

datasplit 931 Stars

**DataSploit**  
Overview  
Setting up the Environment  
[How to Generate Api Keys](#)  
Usage  
Contributors

## How to Generate Api Keys

We need following API keys to run this tool efficiently. - shodan\_api - censysio\_id - censysio\_secret - zoomeyeuser - zoomeyepass - clearbit\_apikey - emailhunter - fullcontact - google\_cse\_key - google\_cse\_cx

### Shodan\_api

- Register an account in shodan.
- Visit your registered email id and activate the account.
- Login to your account and you will find the API keys under profile overview tab.
- Copy the API key and this is the value for *shodan\_api* field in the config.py file.

### Censysio ID and Secret

- Register an account in censysio.
- Visit your registered email id and activate the account.
- Login to your account.
- Visit [Account](#) tab to get API ID and Secret.
- Your API key is the value for *censysio\_id* field and API Secret is the value for *censysio\_secret* field in config.py file.

### Clearbit API

- Register an account in clearbit.
- It will auto redirect to the account.

**Table of contents**  
Shodan\_api  
Censysio ID ar  
Clearbit API  
Emailhunter A  
Fullcontact AF  
Google Custor API key and C  
Zoomeye User Password

https://datasplit.github.io/datasplit/setupGuide/

Setting up the Environment

Search

**DataSploit**  
Overview  
[Setting up the Environment](#)  
How to Generate Api Keys  
Usage  
Contributors

## Setting up the Environment

This page holds the setup guide you will need before kicking off the datasplit in your system. Please note that all the documentation is as per \*nix machines, and the tool has not been thoroughly tested on Windows platform. If you would like to volunteer for the same, give us a shout at helpme@datasplit.info. Following are the quick steps to get you going:

If you want to work with web gui, follow the steps till 7. Otherwise, follow till 5th and you should be good to go.

### Step 1 - Download DataSploit to your system.

You can either use the git command line tools using the following command:

```
git clone https://github.com/datasplit/datasplit.git
```

, or you can simply download the zip file ([link](#)) and extract the same using unzip.

```
unzip master.zip
```

### Step 2: Install python dependencies

Go into the tool directory and install all the python libraries using the requirements.txt file. In case you encounter 'Permission Denied' error, use sudo.

```
cd master  
pip install -r requirements.txt
```

### Step 3: Rename config\_sample.py to config.py



# Output Formats

- HTML
- JSON
- Emails List (txt file)
- Subdomains List (txt file)

```
beaker.ma...com
develop...p.com
inspirat...p.com
mail.adm...com
pizza.ma...com
qa.mailc...com
sc1.mail...com
st1.mail...com
st2.mail...com
stx.mail...com
stxv2.ma...com
wavelengt...com
modev1.ma...com
old-kb.ma...com
mailchimp...com
slgw.mail...com
fastfives...com
fb101.ma...com
```

### DataSploit

Report for mailchimp.com

#### WHOIS Information

```
{
  "updated_date": [
    "2016-01-19 00:00:00",
    "2017-03-05 15:25:01"
  ],
  "status": [
    "serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited",
    "serverTransferProhibited https://icann.org/epp#serverTransferProhibited"
  ],
  "name": "ROCKET SCIENCE GROUP",
  "dnssec": "Unsigned",
  "city": "ATLANTA",
  "expiration_date": [
    "2018-06-29 00:00:00",
    "2018-06-29 04:00:00"
  ]
}
```

#### A Records

23.51.136.95
--------------

#### MX Records

1 aspmx.l.google.com.
10 aspmx3.googlemail.com.
5 alt1.aspmx.l.google.com.
10 aspmx2.googlemail.com.
5 alt2.aspmx.l.google.com.

#### SOA Records

```
file:///Users/shubhammittal/Documents/Pythoncodes/datasploit_parent/datasploit/reports/mailchimp.com/mailchimp.com_2017
{"wappalyzer": {"http": [u'\tGoogle Analytics', u'\tGoogle Tag Manager'], "https": [u'\tGoogle Analytics', u'\tGoogle Ta
9f58...
u' 30
12-3
Leng
u' lo
29T2
u' <h
u' lo
{u'o
u'pr
u'de
301
stat
u'po
u'ti
bgco
6166
u' 82
u'city': u'Deatur', u'region_code': u'CA', u'area_code': 404, u'longitude': -84.283, u'country_code?': u'USA', u'country_name': u'United Sta
```

```
hello@ma...
legal@ma...
abuse@ma...
laurissa...
imports@...
talent@...
mobilehe...
pr@mailc...
colors@...
dan@mail...
john@mai...
gregg@ma...
help@mai...
shirts@...
wordpres...
tara.sha...
shopify@...
support@...
info@mai...
api@mail...
apibeta@...
ecommerc...com
contact@...
examples...imp.com
template...p.com
customer...p.com
domains@...
kate@mai...
twitter@...p.com
accounts...p.com
agencies...om
whatsins...om
apiconne...
tedx@mai...
biz@mail...
salesfor...
dev@mail...
apihelp@...imp.com
```



**DEMO TIME**



**LET'S HOPE THE DEMO-GODS ARE  
SMILING!**

# Twitter: @datasplit

<https://twitter.com/datasplit>

https://twitter.com/datasplit

Home Notifications Messages Search Twitter

**DataSplit**  
Open Source Assistant for #OSINT

**datasplit**  
@datasplit FOLLOWS YOU  
Open Source Assistant for #OSINT  
[github.com/upgoingstar/dasplit](https://github.com/upgoingstar/dasplit)  
Joined July 2016

Tweet to Message

20 Followers you know

Photos and videos

TWEETS 196 FOLLOWING 110 FOLLOWERS 406 LIKES 25

Tweets Tweets & replies Media

datasplit Retweeted  
**amticker.de** @amtickerde · 12h  
Collection Of Open Source Intelligence Resources  
[amticker.de/collection-of-...](https://amticker.de/collection-of-...) #amtickerde

Collection Of Open Source Intelligence Resources -...  
Wichtige Informationen zum Thema Collection Of Open Source Intelligence Resources. Besuche unsere Seite noch heute!  
amticker.de

datasplit Retweeted  
**Shashank shekhar** @Shankywit · 5h  
3 Advantages of Using an Open Source Business Intelligence Tool  
[paper.li/Shankywit/1465...](https://paper.li/Shankywit/1465...) Thanks to @\_crowdreviews\_  
#businessintelligence

Browser address bar: <https://www.facebook.com/datasploit/?ref=ts>


Navigation bar: Cloud, The Configuration Sy, SensePost | Revistin, Offensive Security Bl, Python Tools : Penet, Encoding Web Shells, enjoiz/XXEinjector: T, Rapport d'au

Facebook Page Header: DataSploit, Search, Shubham, Home 20+, Settings, Help

Page Navigation: Page, Messages, Notifications, Insights, Publishing Tools

Profile Card: DataSploit, Open Source Assistant for #OSINT

Post 1: DataSploit, Published by Twitter [?] · August 1 at 4:43pm ·   
Retweeted Ahmed AlHamli (@AhmedAlHamli):  
Big Data and open source intelligence – A game-changer for counter-terrorism? <https://t.co/cHZO7SeZGu>



Big Data and open source intelligence – A game-changer for counter-terrorism? | TRENDS  
The threat from terrorism continues to present a clear and present danger to many communities across the world. The suicide bombings in Turkey on 28th June which...  
TRENDSINSTITUTION.ORG/?P=2019

13 people reached Boost Post

Like Comment Share

Post 2: DataSploit, Published by Twitter [?] · August 1 at 4:43pm ·   
Retweeted Steven Hager (@stevenhager420):  
A Brief History of Open Source Intelligence - bellingcat  
<https://t.co/uzzyAKAtRM>

PHOTOS: DataSploit Overview: 

- Performs automated OSINT on a domain / email / out relevant information from different sources.
- Useful for Pen-testers, Cyber Investigators, Product security professionals, etc.
- Correlates and collaborate the results, show them
- Tries to find our credentials, api-keys, tokens, session legacy portals, etc. related to the target.
- Available as single consolidating tool as well as s
- Available in both GUI and Console.

UPCOMING EVENTS: Create events for your Page. Create Event

VISITOR POSTS: Be the first to add a post

# Facebook: /datasploit

<https://www.facebook.com/datasploit/>

# Roadmap

- Allows to set up periodic scans and alerting for product security companies.
- Intelligence on co-relation and identity verification.
- Reports in CSV.
- Reverse Image Search and profile validation.
- Works closely with various social network APIs.
- Refine Pastebin and Github Searches.
- IP Threat Intelligence.
- Organization Scoping.
- Integration with SE other tools.
- Cloud related OSINT and active modules.
- pip install datasplloit (to be installed as both library as well as script)



# Coverage



CircleCityCon 4.0

OSINT Framework





# How to Contribute

- Help us in testing the tool
- Expand : Write/Suggest modules
- Give Feedback: raise issues, tweet, drop an email.
- Use / Promote / Write about the tool.
- Write OSINT blogs / tool walkthrough(s) / etc.
- Report issues at <https://github.com/dataspl0it/dataspl0it/issues>

# Core Contributors.

- Shubham Mittal (@upgoingstar)
- Nutan Kumar Panda (@nutankumarpanda)
- Sudhanshu (@sudhanshu\_c)
- Kunal (@KunalAggarwal92)
  
- Kudos to
  - @anantshri for mentoring.
  - @ bnchandrapal for feedbacks, suggestions and other help around issues.

# Thanks. g0t questions?

<https://github.com/DataSploit/datasploit>

Follow [@datasploit](#) for OSINT news and latest updates.

Tweet / DM to **@datasploit**

upgoingstar@gmail.com

