LinkedIn reconnaissance tool

30 commits 1 branch 0 packages 0 releases 1 contributor

Branch: master New pull request Find file Clone or download

arch4ngel refinements Latest commit c7fc475 6 days ago

Peasant	refinements	6 days ago
.gitignore	adding gitignore	4 months ago
README.md	Update README.md	10 days ago
invitations.py	adding tool to extract sent invitations	3 months ago
peasant.py	refinements	6 days ago
requirements.txt	updates	23 days ago

README.md

Peasant

Brought to you by:

Peasant is a LinkedIn reconnaissance utility written in Python3 that functions much like LinkedInt by @vysecurity. It authenticates to LinkedIn and uses the API to perform several tasks.

- Profile information harvesting
- Automated connection requests
- Profile spoofing, i.e. update your profile with the content of another

Output from profile harvesting is provided in CSV format for simple processing. The following output was extracted when targeting the `dundermifflindesign` profile:

```
first_name,last_name,occupation,public_identifier,industry,location,entity_urn,company_name,company_id,con
Paul,M,Quality Assurance Specialist at Dollar General,paul-m-04773b1,Government Administration,Greater Pit
,,"VP of Sales at Dunder Mifflin Design Company, Inc.",UNKNOWN,Graphic Design,Greater St. Louis Area,ACoAJ
```

Requirements

Note: I intend to create a Docker image for this eventually ...but until then

Peasant requires Python3.7 or greater. If on Debian, Use the following command to install dependencies:

```
python3 -m pip install -r requirements.txt
```

Usage

Profile Harvesting

By supplying one or more company names to the `harvest` command, Peasant will make API calls to acquire the numeric identifier of a target company identifier and proceed to enumerate employees from the people section of the target company.

Example

If the target is Dunder Mifflin Design and the company name was found to be `dundermifflindesign` via search engine, then the following command would attempt to harvest profiles and write CSV records to dundermifflin.csv:

WARNING: Use of the `-ac` flag will result in a connection request being sent to each accessible profile. If you wish to filter for particlar profiles, use the `-of` flag to dump the results to disk and select specific records via grep and use the `add_contacts` subcommand to create connection requests.

```
archangel@deskjet~~> export creds='username_here:password_here' # or interactive authentication
archangel@deskjet~~> ./peasant.py harvest -C "$creds" -cns dundermifflindesign -of dundermifflin.csv

    //   ) )
   //___/ /  ___      ___      ___      ___       __    __  ___
  / ____ / //___) ) //   ) ) ((   ) ) //   ) ) //   ) )  / /
 //       //       //   / /   \ \    //   / / //   / /  / /
//       ((____   ((___( ( //   ) ) ((___( ( //   / /  / /

[+] Starting new CSV file: dundermifflin.csv
[+] Authenticating session
[+] Authenticated as a premium subscriber
[+] Company Identifier for dundermifflindesign: 19067092
[+] Getting initial profiles
[+] Available profiles: 101
[+] Logging out of LinkedIn
[+] Writing output to dundermifflin.csv
[+] Done!
[+] Logging out
[+] Done...exiting
```

Limitations

LinkedIn will allow only the first 1,000 search results to be returned when harvesting contact information, however the same results are not returned each time a series of searches are applied. Run the harvest command multiple times to capture more contacts.

Here are two ways to increase the number of contacts a given profile can access:

1. Generate connection requests for company people via the `add_contacts` subcommand or the `-ac` flag of the `harvest` command

2. Update the target profile such that you are in a position at the target company. This appears to facilitate access to more contacts initially.

Connection Request Generation

Use the `add_contacts` subcommand to generate connection requests for target profiles. This command takes the name of a CSV file generated by the `harvest` subommand and will indiscriminately send a connection request for each record.

Example

To send a connection request to each of the profiles enumerated from Dunder Mifflin, run the following command. After execution, visit the `My Network` tab of your LinkedIn profile to observe the connection requests.

Bonus: Use the `-m` flag of this subcommand to send a custom message to the receipients, just be aware that this is still being tested.

```
archangel@deskjet:peasant~> ./peasant.py add_contacts -if dundermifflin.csv -C "$creds"

    //   ) )
   //___/ /  ___      ___      ___      ___       __    __  ___
  / ____ / //___) ) //   ) ) ((   ) ) //   ) ) //   ) )  / /
 //       //       //   / /   \ \    //   / / //   / /  / /
//       ((____   ((___( ( //   ) ) ((___( ( //   / /  / /

[+] Loading CSV file: dundermifflin.csv
[+] Total profiles loaded: 2
[+] Authenticating session
[+] Authenticated as a premium subscriber
[+] Sending connection requests, which will take some time...
[+] Sending Connection Request 1:  , VP of Sales at Dunder Mifflin Design Company, Inc. @ dundermifflindes
[+] Sending Connection Request 2: Paul M, Quality Assurance Specialist at Dollar General @ dundermifflinde
[+] Writing profiles to file: dundermifflin.csv
[+] Logging out
[+] Done...exiting
```

Profile Spoofing

Use the `spoof_profile` command to spoof basic profile information, along with education and experience from a target profile back to the one associated with credentials passed at the command line. This is useful during social engineering engagements where impersonating a profile may enhance legitimacy of a pretext. The target profile is selected by using the publicly available profile label found on the profile page.

Warning: This command only spoofs textual information. Images will need to be extracted and applied accordingly.

Double Warning: This will permanently overwrite the content of the authenticated profile with that of the target profile.

Example

The following command could be ran to spoof the profile of Paul M. at Dunder Mifflin. After execution, review the authenticated profile and observe that it has been updated with the information from the target profile.

```
archangel@deskjet:peasant~> ./peasant.py spoof_profile -pu paul-m-04773b1 -C "$creds"

    //   ) )
   //___/ /  ___      ___      ___      ___       __    __  ___
  / ____ / //___) ) //   ) ) ((   ) ) //   ) ) //   ) )  / /
 //       //       //   / /   \ \    //   / / //   / /  / /
//       ((____   ((___( ( //   ) ) ((___( ( //   / /  / /

[+] Authenticating session
[+] Authenticated as a premium subscriber
[+] Spoofing basic profile information...
[+] Clearing current profile education and spoofing target content...
[+] Clearing current profile experience and spoofing target content...
[+] Logging out
[+] Done...exiting
```