MALTEGO

INTEGRATING 'HAVE I BEEN PWNED' DATABASE WITH MALTEGO TO FIND EMPLOYEES CREDENTIALS LEAKS IN A DOMAIN

CREATED AND EDITED BY: TAMIR MAIDANI

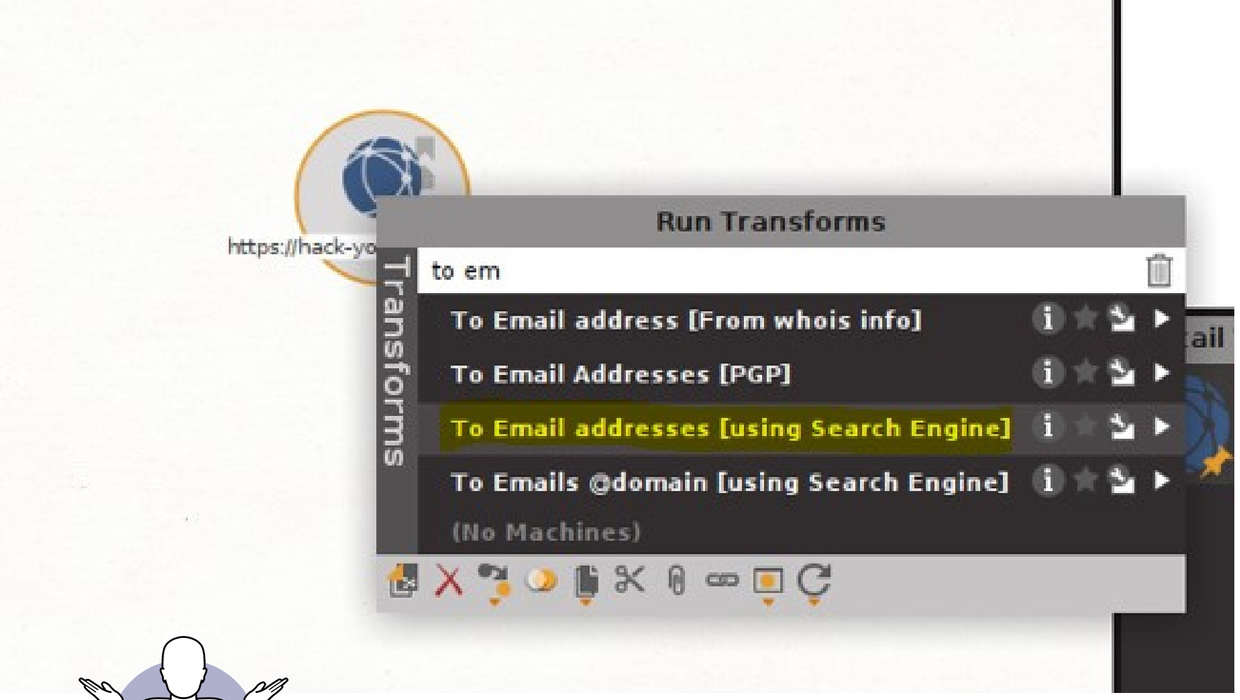
INVESTIGATION OBJECTIVE

in every company/organization every CEO wants to know that the information of the company
and employees credentials remains safe.
for that ,the company needs to keep a strict policies about sharing information out to the public
and to increase the awareness of the company employees about the different risks in the protective measures that
can be done with regards to information spreading on the web.
but in case the CEO or security team has a suspicion about information that's already was leaked and a reckless behavior from the
employees side , it is important to check where is the 'main source' of the problem
and what specific details was already 'out to the world',
for that we can conduct an OSINT investigation with maltego,
in our case we will conduct the osint investigation on 'hack-your-self-first' website

Important Note!

'hack-your-self-first' domain is platform that's allow all to hack the site and to conduct an OSINT investigation on it,
always check before with the owners of the domain if you have the right Permissions to do so

STEP 1

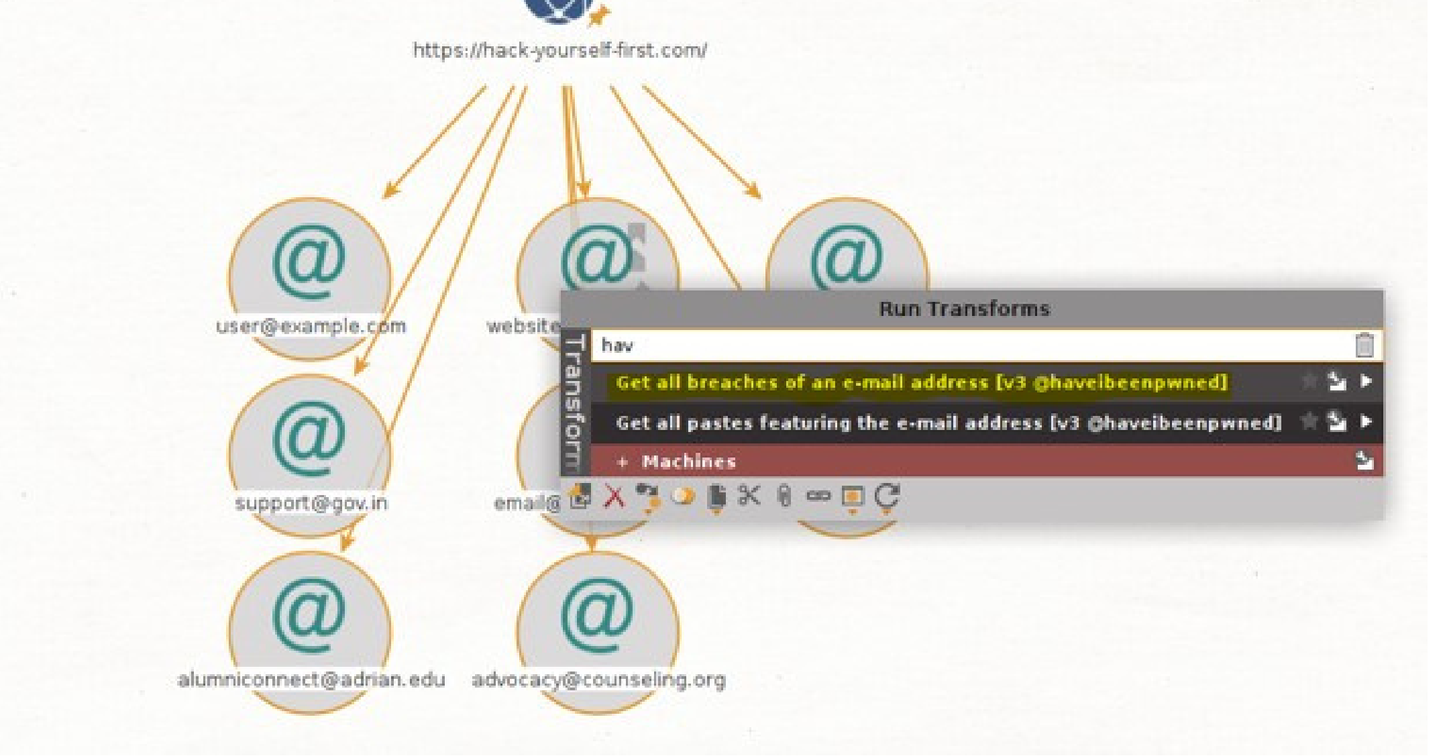


we need first to choose a domain and pull it to the screen -- right
after we will use our first transform,
we will search the 'to email address'(using search engine)
in order to search employees emails

WHAT ARE TRANSFORMS?

RESULTES

we found several employees emails ,
which only in this point we saved ourselves
a long searching effort with different osint tools.



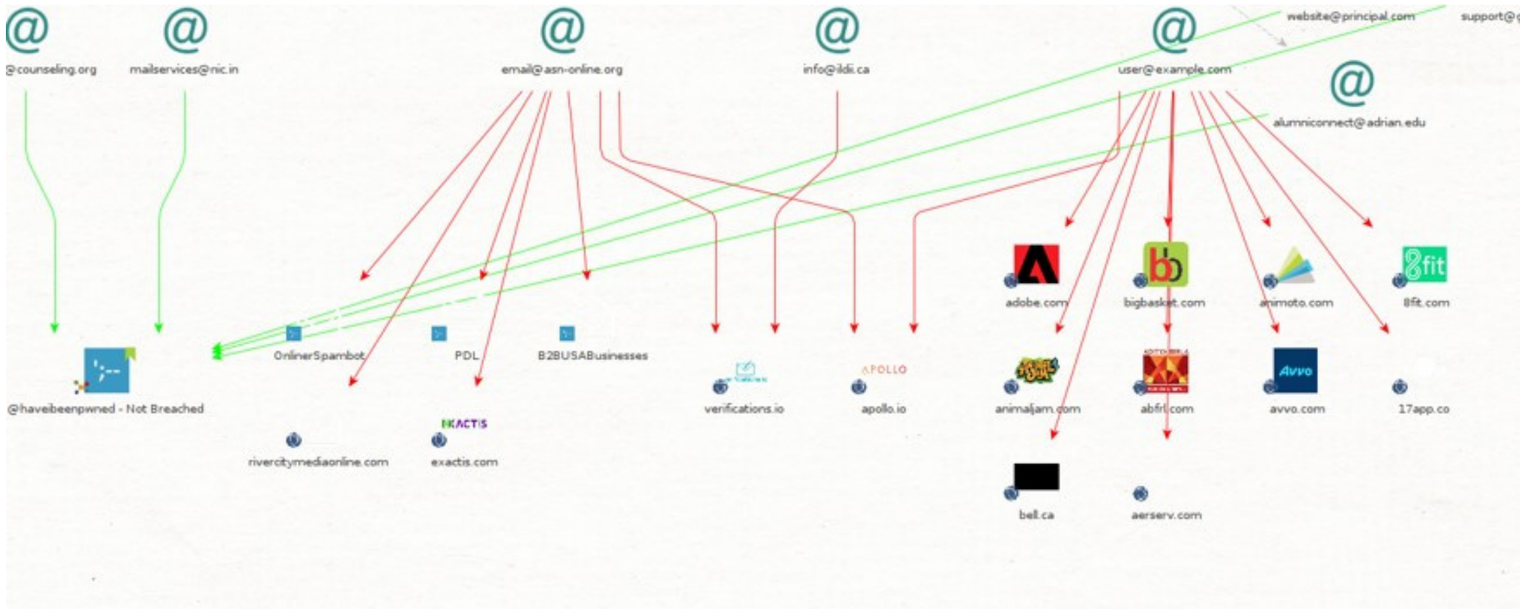
STEP 2

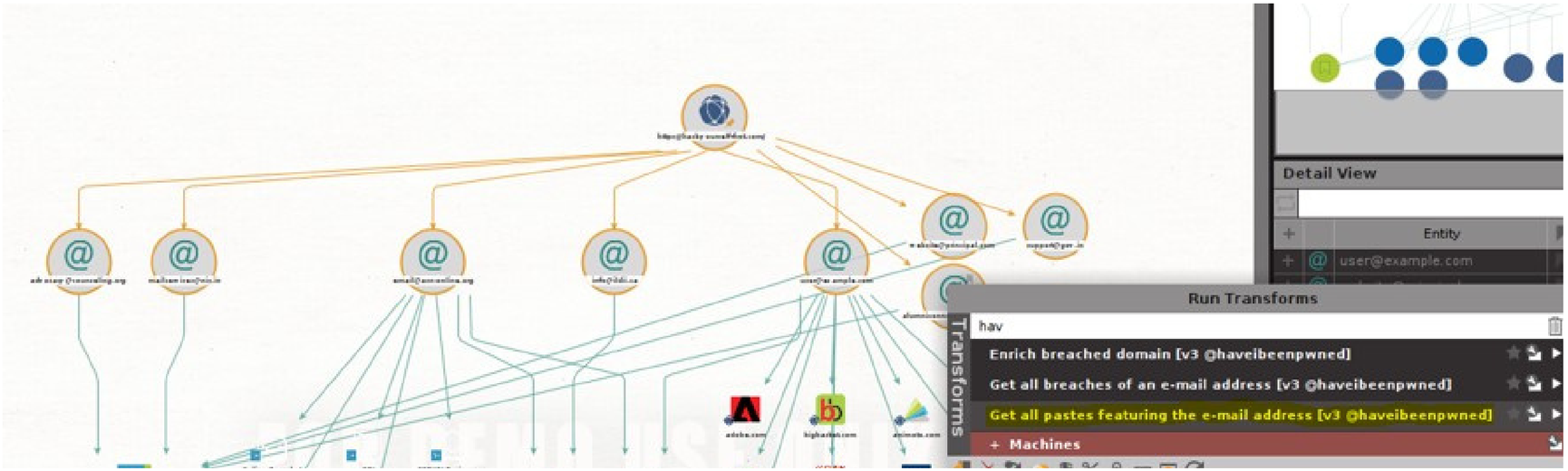
now there is 2 ways that employees got their credentials stolen :
1.data breach in a third-party who olds employees credentials
2.pastebin- a place who someone "throw" someone else stolen credentials
we want to check the 2 options -- for that we will be using 'have i been pwned' database.
by using search bar for 'have i been pwend'
first we will use the **first 'breach' transform -- 'get all breaches'**

RESULTES

we found some of employees data breached by some services.
that employees may have been registered for that services in the past.

WHAT IS 'HAVE I BEEN PWNED' DATABASE?





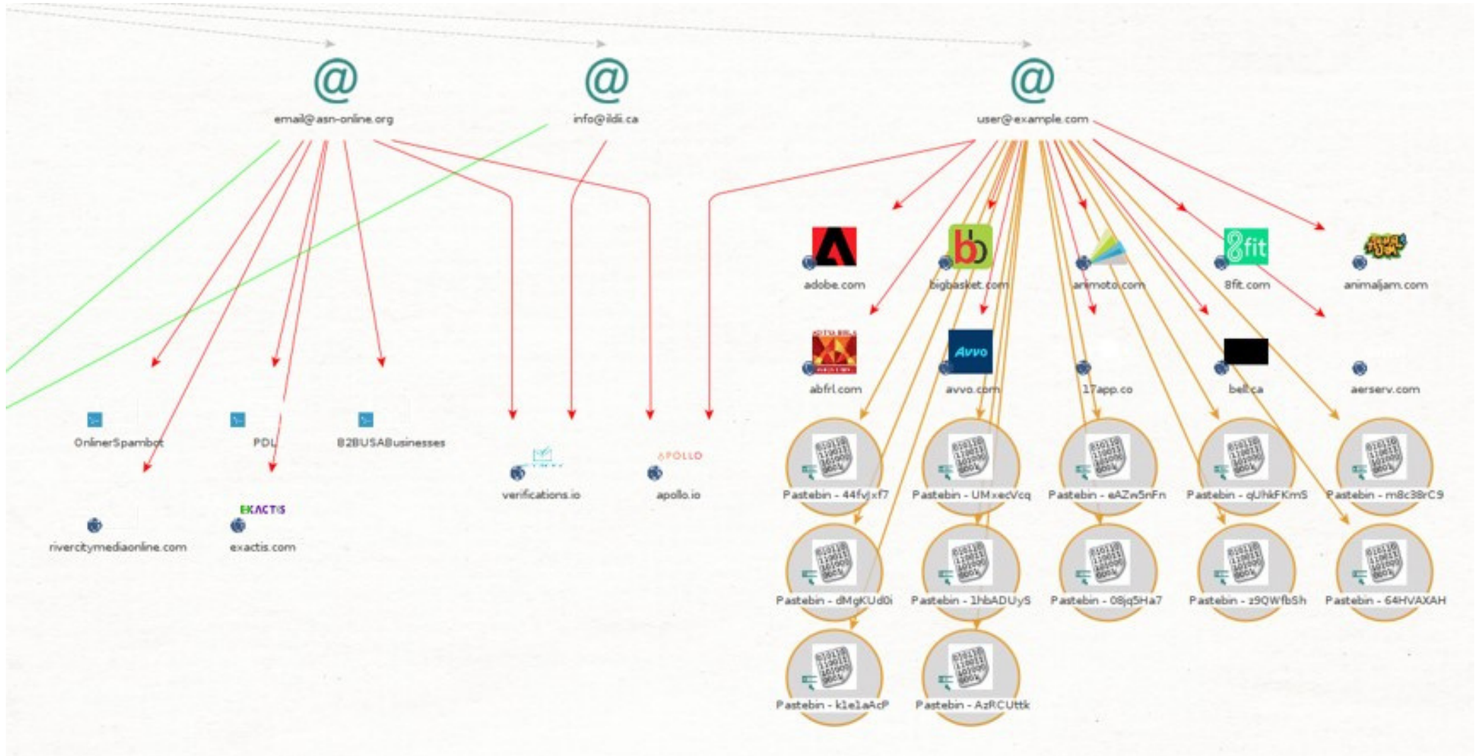
STEP 3

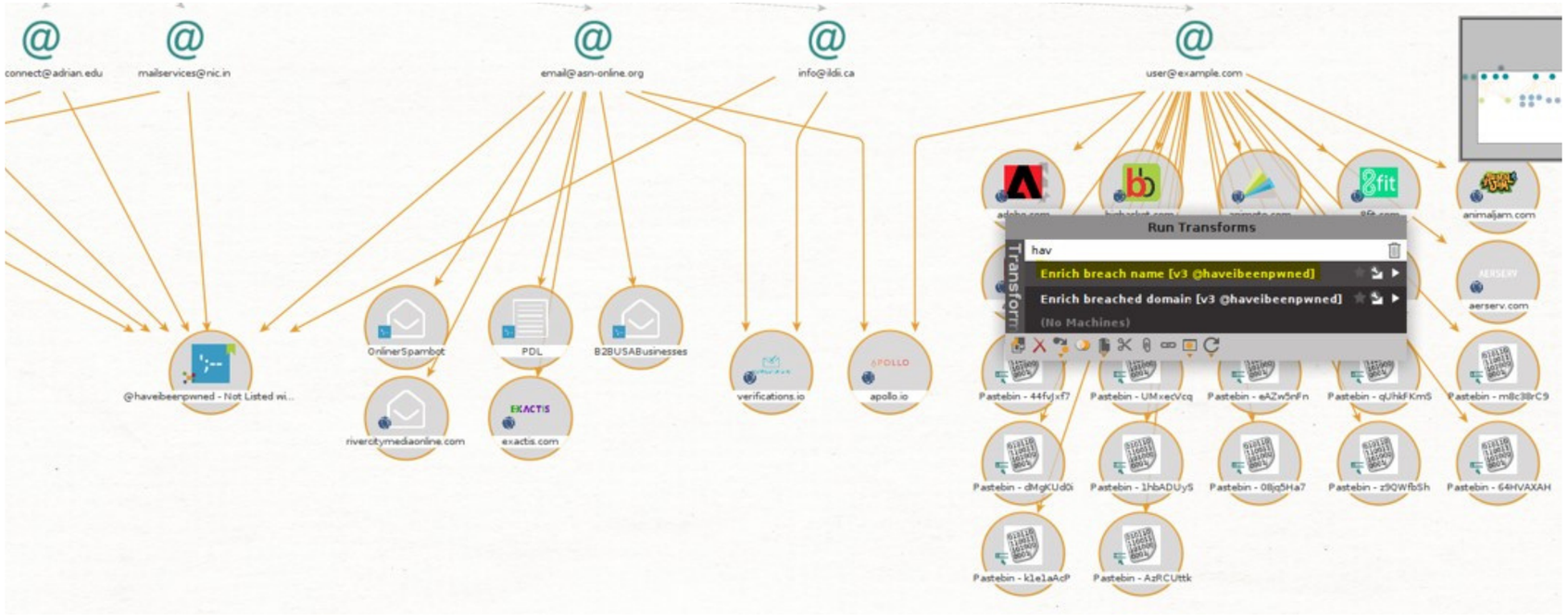
now lets check for pastebin leaks-- 'get all pastes'

MORE ABOUT 'PASTEBIN'?

RESULTES

we can see we got links to a pastebins pages that shows that the data of the employees is found there.





STEP 4

in the end we want to know what specific data has been compromised from every emploee --
so we will run the last transform -- we will mark all of our outcome by selecting all of it and then choosing -- 'enrich breach name'

RESULTES

and now we can see what information for every emploee has been leeked