CYBER FORENSIC T20 SERIES

"INVESTIGATING ROMANCE SCAMS WEBSITE/PROFILES"

SUPPORTED BY MALTEGO

The poster is made to present the Forensic Investigation work on problem statement "Investigating Romance Scam Website/Profiles" using Maltego tool. The Cyber Forensic T20 Series has been conducted Under Vellore Institute of Technology, Vellore, in collaboration With Maltego.

Authors

This Work is done by Moulik Singh Arora (20BIT0415), Preksha J Dadhania (20BIT0158), Vineet Jain (20BIT0342)
Information Technology, B.tech, VIT University, Vellore, TamilNadu

Advisors and Department

This work is Submitted to Dr. Priya V,(SITE) Dr. Sumaiya Thaseen(SITE) and Maltego team. We thank you all to give us the opportunity to work under you.

INTRODUCTION

- .With the increasing technology it has become even more difficult to authenticate the messages sent by a person. Many cases of people being scammed online in the name of love have surfaced.
- We are addressing the issue of investigating romance scam websites/profiles using Maltego tool. Maltego is an information gathering tool which is widely used for forensic investigation.

OBJECTIVE

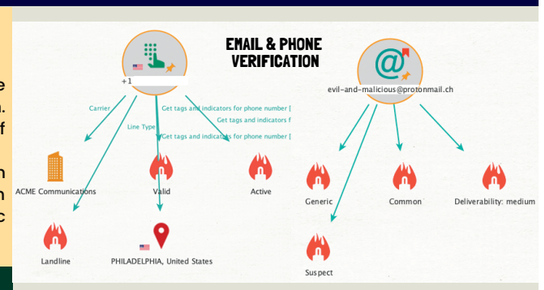
- Our objective is to investigate romance scam profiles and website using maltego with the help of various transforms. We are trying to differentiate between real and fake users based on the results.
- Additionally we are trying to suggest different scripts that can be taken as initiatives to prevent romance scams.

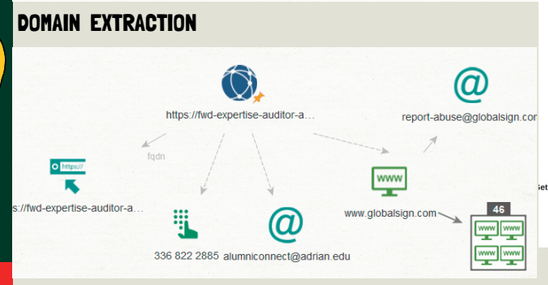
SOCIAL IMPACT

- This work has been done to find out the relation between real account and fake account and to investigate about the user associated with romance scam using maltego tool.
- Finding information about the culprit helps to safeguard victims from being scammed by attackers.

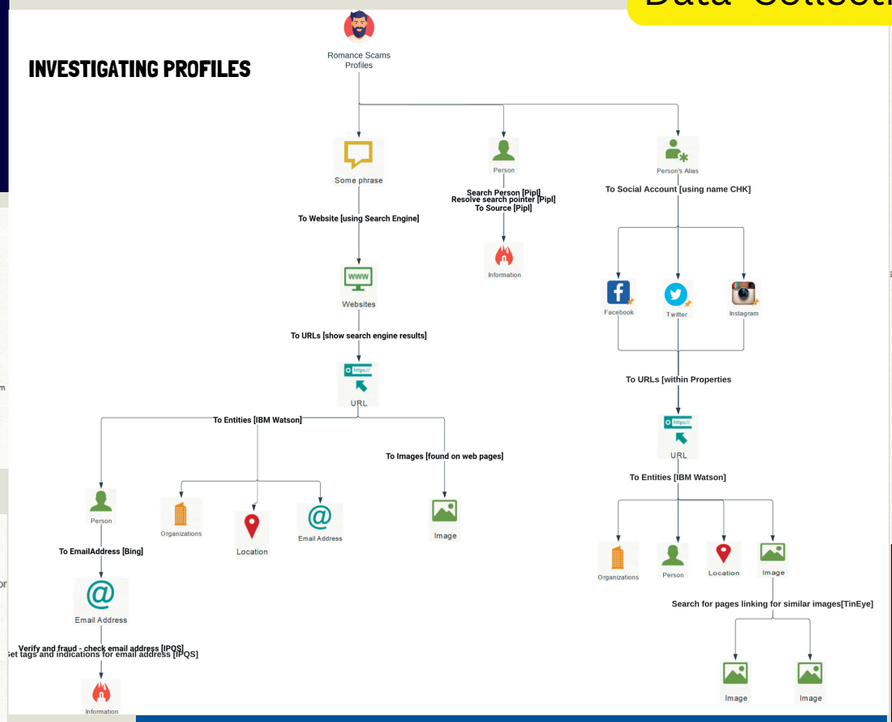
METHODOLOGY

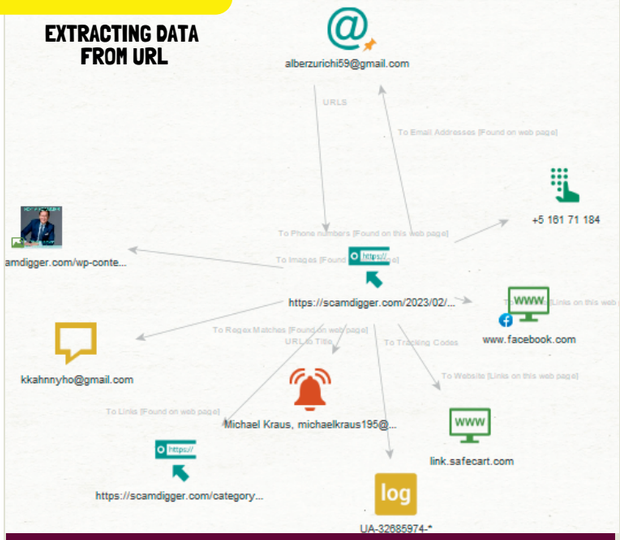
- Data collection from opensource websites like romancescam.com, scamdigger.com and from maltego using phrase entity and tried to find some scam websites.
- We used multiple transforms which include Standard transform, email url to website, SSL certificate, To emailAddress[bing], IPQS, to social account[using name CHK] and few phrases such as romance fraud, dating scams, and golddigger.
- We implemented algorithms on dataset to get the probability of a profile being fake. Future works can include methods that can be used to reduce or prevent scams at larger aspect.

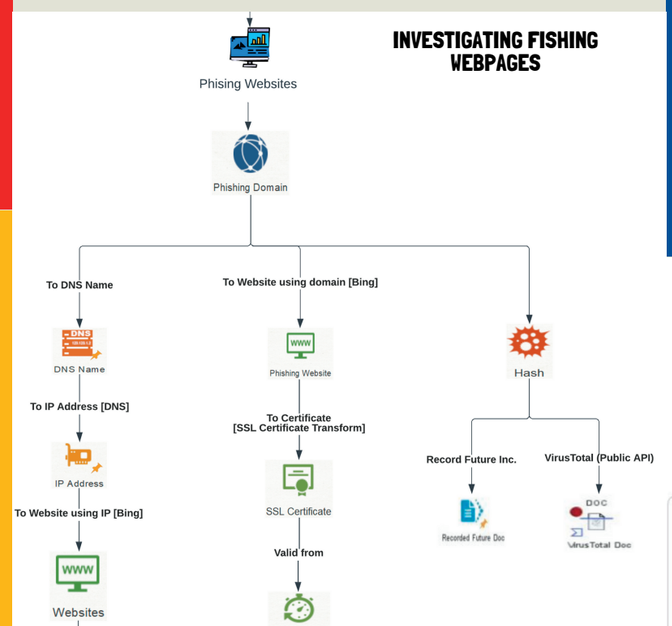




Data Collection Process



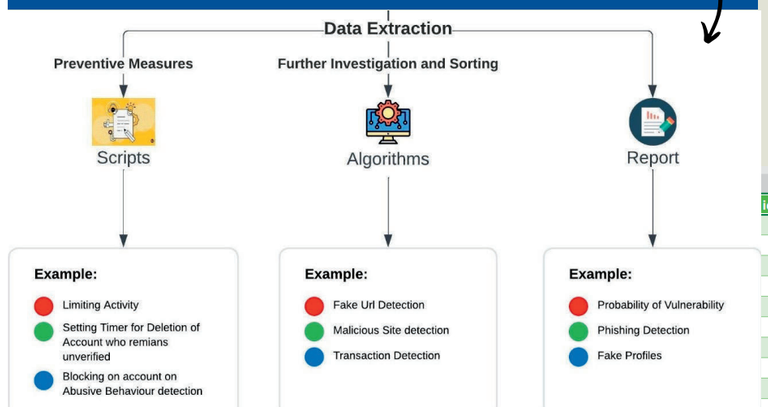




FUTURE WORK/RESEARCH:

According to our studies we also observed many gaps in security of certain portals which can be enhanced by implementing few scripts or parameters that have been suggested below.

- Mobile Number should be collected during account creation and re-verification should be done after 1 day.
- Minimum 2 images of user should be collected during profile building stage to improve authenticity.
- Scripts should be used to detect human presence while uploading images to avoid spam pictures.
- Auto block feature to temporarilily block accounts which send bulk messages.
- Abusive Key phrases/External link redirection alert should be created



RESULTS/CONCLUSIONS

- Obtained results are in different forms using which we try to find out the probability of a website and profile being fake.
- We observed that most of the fake profiles uses the genuine images of other users who are unaware about their picture being used in other portals. Temporary email IDs are also being used while creating account on dating websites. Hence romance websites lack security parameters.
- While investigating, we tried to analyze the pattern of attack and how a victim thinks while creating an account, thus we have proposed few security parameters for future works.

	A	B
1	Email	Ip Address
2	lucasmichadam@gmail.com	69.31.50.51
3	perpetualamoako44@gmail.com	197.251.175.38
4	frankthompson909@gmail.com	180.74.232.185

	A	B
1	Source Entity	Target Entity
2	ahrefs.com	ahrefs.canny.io
3	ahrefs.com	ahrefscomthumbnail-3b70.kxcdn.com
4	ahrefs.com	analytics.ahrefs.com
5	ahrefs.com	analytics.ahrefs.com,

A	B	C	D	E
id	name	screen_name	statuses_count	followers_count
370098498	pirfectmoses	pirfectmoses	24	4
37384589	SAK Nair	bsknair1967	656	57
72110028	Deepak	dedjven	1234	15
82885728	Marcos Vinicius	BrowAlves	573	14
110120789	Shri Kant Kanaujia	kanaujiask	675	18
134435538	Shree vishnu.M	shreeswara	1333	73
195913271	crystyane	crystyanesouza	99	26
252647855	shashank shukla	creativebugg	553	63
290499654	santosh nayak	santoshnayak1	1576	8