# HONEYPOT USING AI

By team Xenomorphs: Amisha, Amulya, Anukriti

Random URLs present over the network  have high possibility to hold malicious behaviour.

These malicious URLs are designed in such a way that they lure people to click on them in social media pages and eventually steal confidential data.

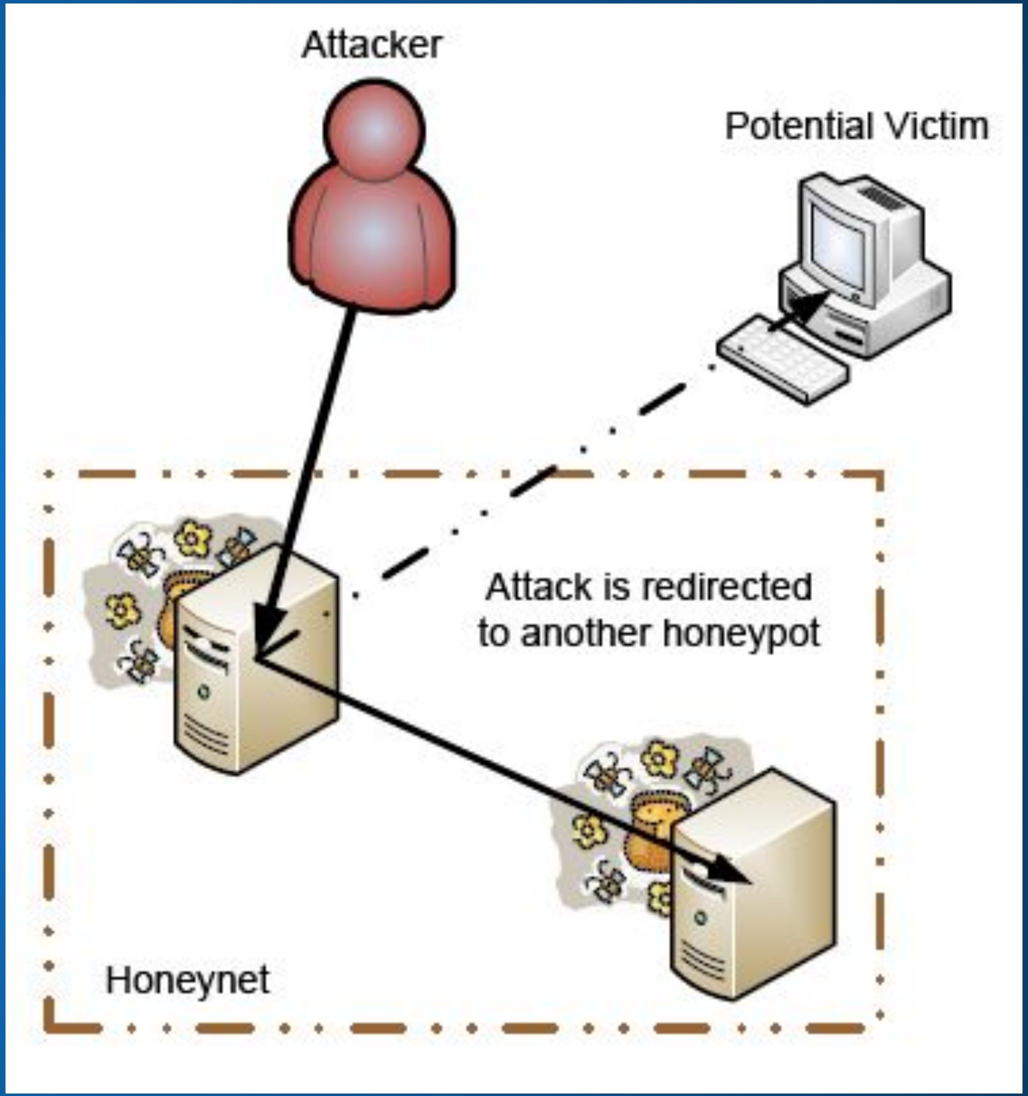
For example : Phishing Attack

# HONEYPOT

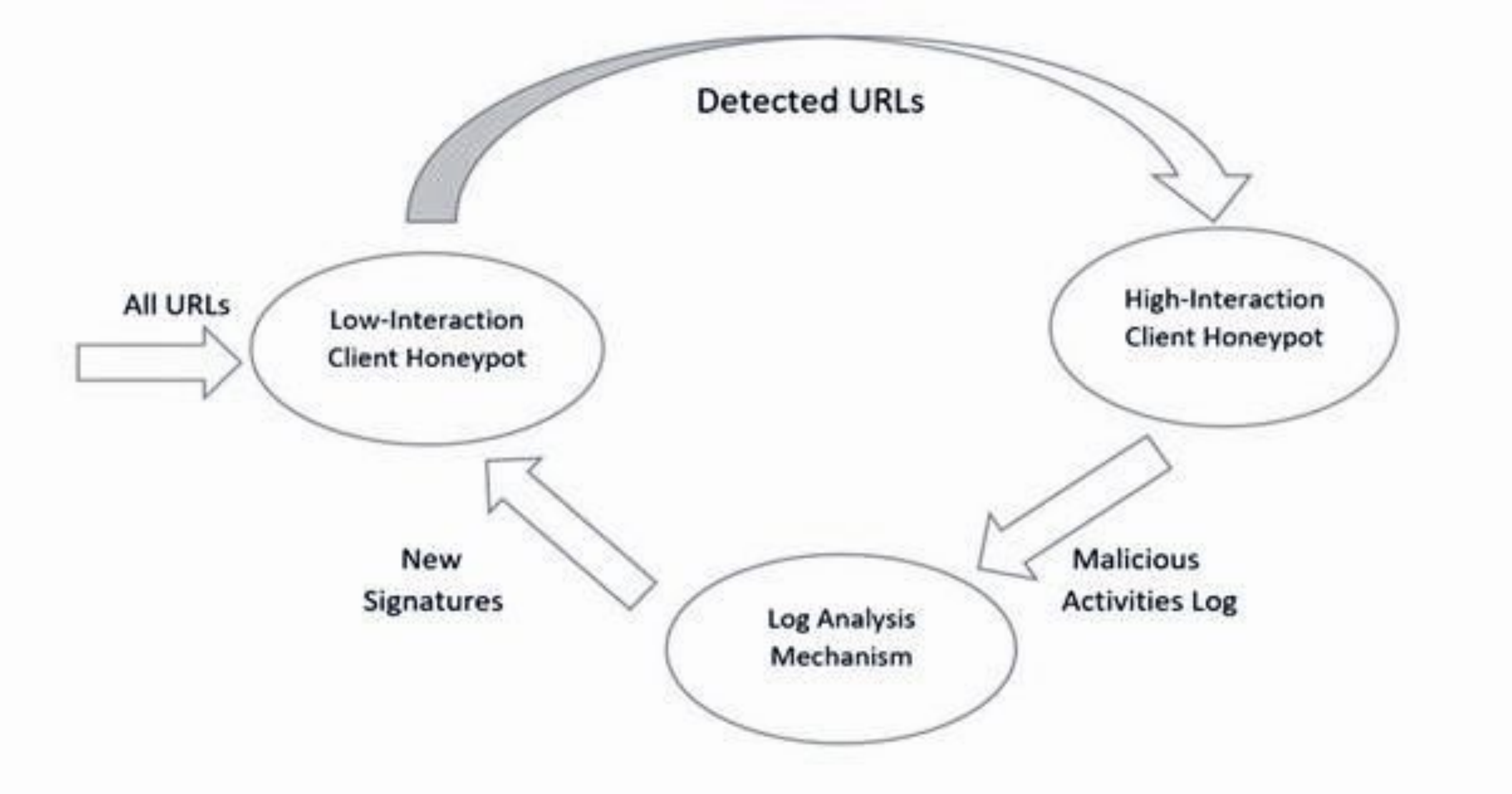
Existing methods to prevent this kind of attacks is the use of honeypots but they still have some loopholes/vulnerabilities which attackers take advantage of.
There are various kinds of honeypots of which some specialize in only detecting while others do a deep scan of attackers whereabouts.

There is a constant need of enhancing our system So that it could cope up with the new and upcoming attacking scripts.

Hence, our aim is to create an Analysis model to enhance the existing honeypots using AI for it to work even more efficiently.

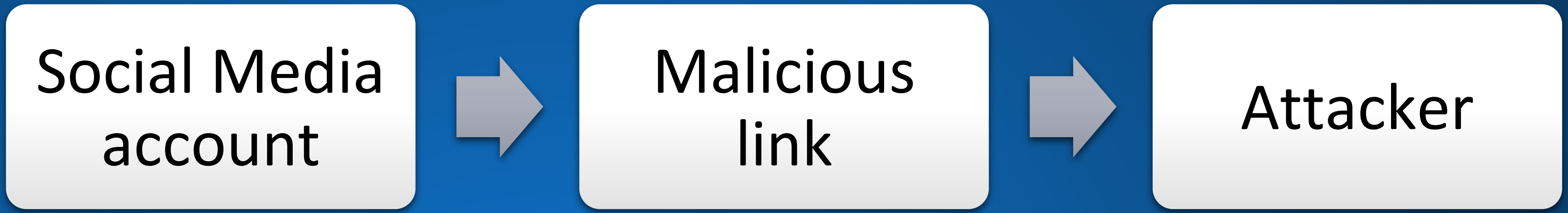


# Our Analysis Model of Honey pot using AI



Reference: Applying AI to Improve the Performance of Client Honeypots Van Lam Le, Peter Komisarczuk, Xiaoying Sharon Gao School of Engineering and Computer Science, Victoria University of Wellington P.O. Box 600, Wellington 6140, New Zealand

WHAT HAPPENS
(layman representation) :



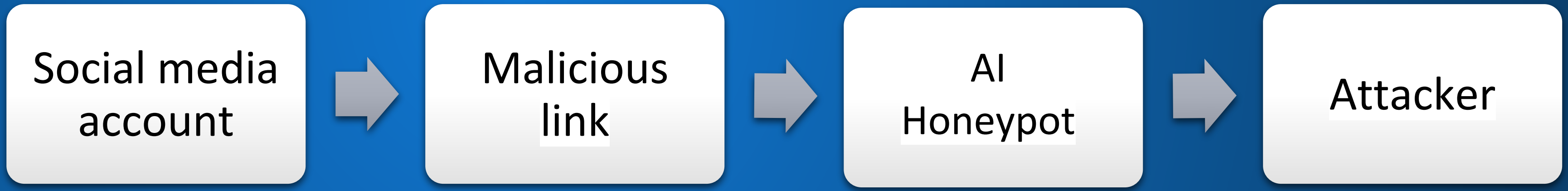
Social Media account

Malicious link

Attacker

AI
Honeypot

OUR IMPLEMENTATION :



Social media account

Malicious link

AI Honeypot

Attacker

- Malicious links may change their codes and it is difficult to be identified by traditional antivirus methods hence we use the machine learning technique to learn the new malicious codes.

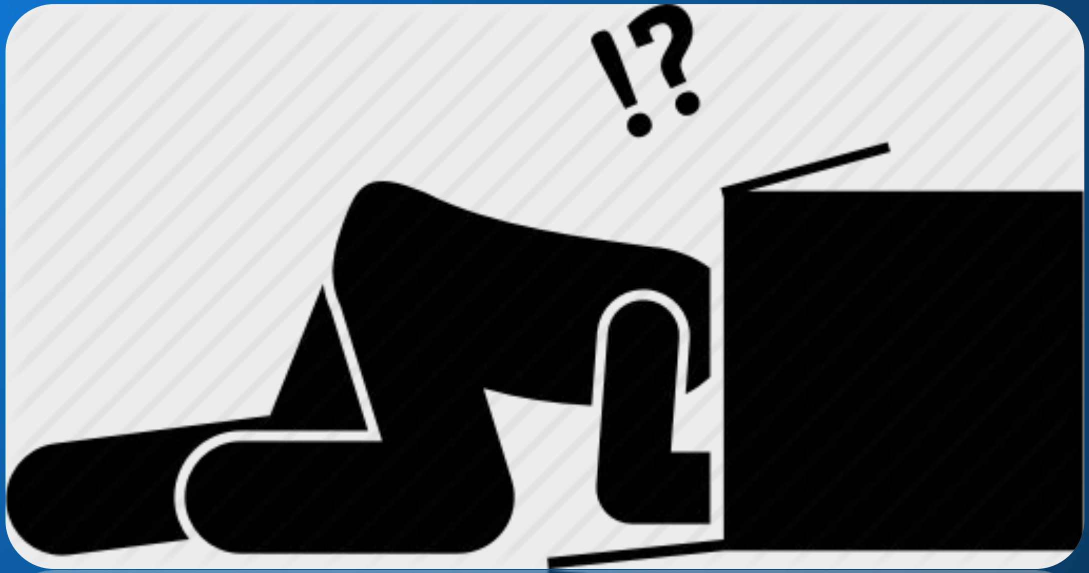
The implementation of AI honeypot shall be done from the server end of any social media page.

# 1$^{st}$ level : Low Interaction Client Honeypot

## WHAT IT DOES?

Low interaction honeypot detects malicious behaviour.
The new plugins which are implemented according to our analysis model are:

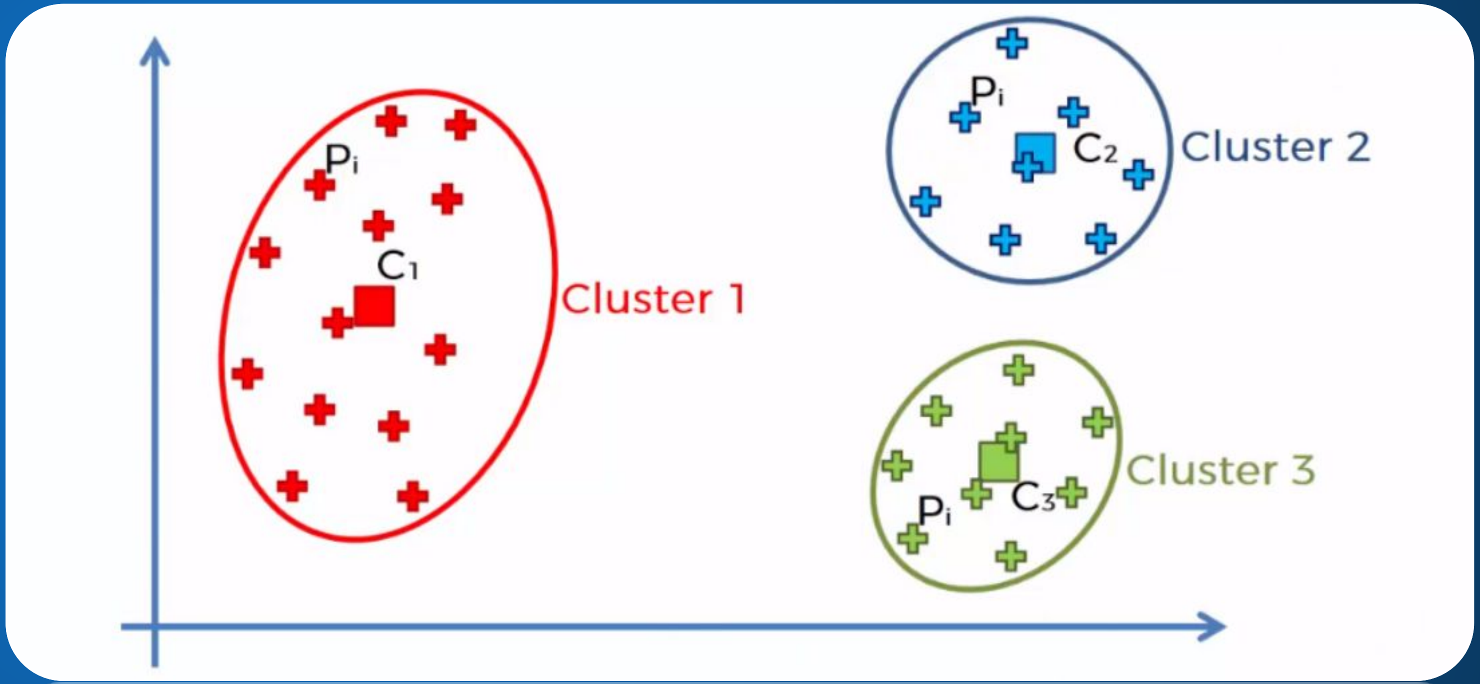
1. It passes to the malicious link to the high interaction honeypot.
2. The log files which are generated from high interaction honeypot is used by low interaction honeypot to enhance its  functionality.



# 2nd level : High Interaction Honeypot

The malicious links which are coming from low interaction honeypot are used as data inputs in high interaction honeypot.

<u>Working of high interaction honeypot:</u>
Data inputs are used in the high interaction honeypot for performing K-means Clustering method to cluster different behaviors in categories/groups in order to study the similarity between all the malicious codes and create it’s own logs for new signatures used again, next time a new malicious URL is trying to penetrate the network.



# CREATION OF LOG FILES

## Composition of Algorithms :

This is a process of combination of  N no. of algorithms in a single function. This means that the analysis of every algorithm is stored as data in respective variables and ultimately averaging the characteristics to create a cumulative log.

$$a(x) = \frac{1}{N} \sum_{n=1}^{N} d_n(x).$$

Where,
a(x) = variable of Xth no. of function
N = no. of algorithms
dn(x) = function of x

# CONCLUSION

This cycle repeats and as a result the system keeps on enhancing itself by logging the new malicious behaviours into its directory and eventually using it as signatures to detect new and innovative attacking scripts/codes.

**THANK YOU!**