HONEYPOT USING AI

Random URLs present over the network have high possibility to hold malicious behaviour.
These malicious URLs are designed in such a way that they can get access to our social media pages and eventually steal confidential data.

Network Among Us!

Malicious Imposter

Client/server

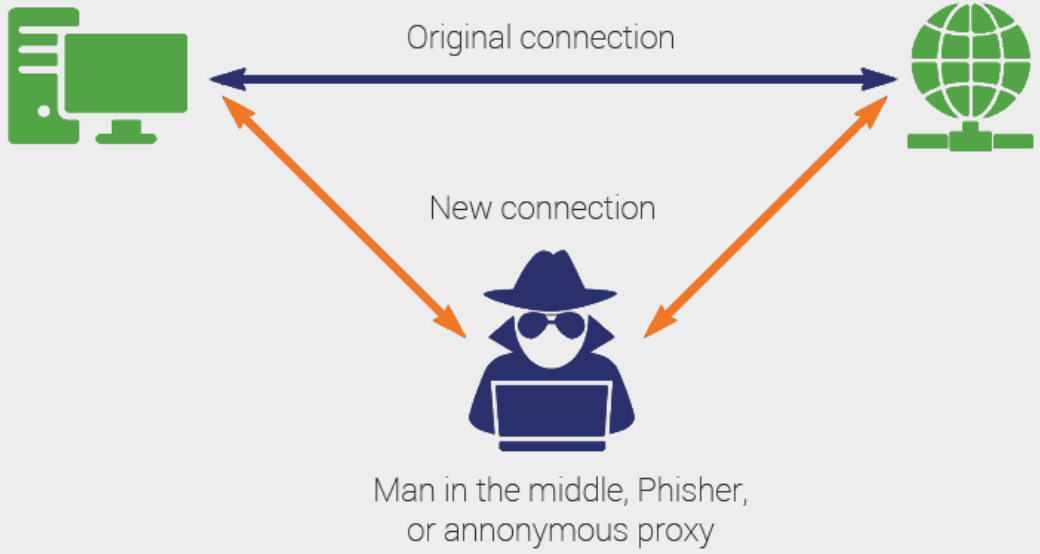
Internet

Client/server

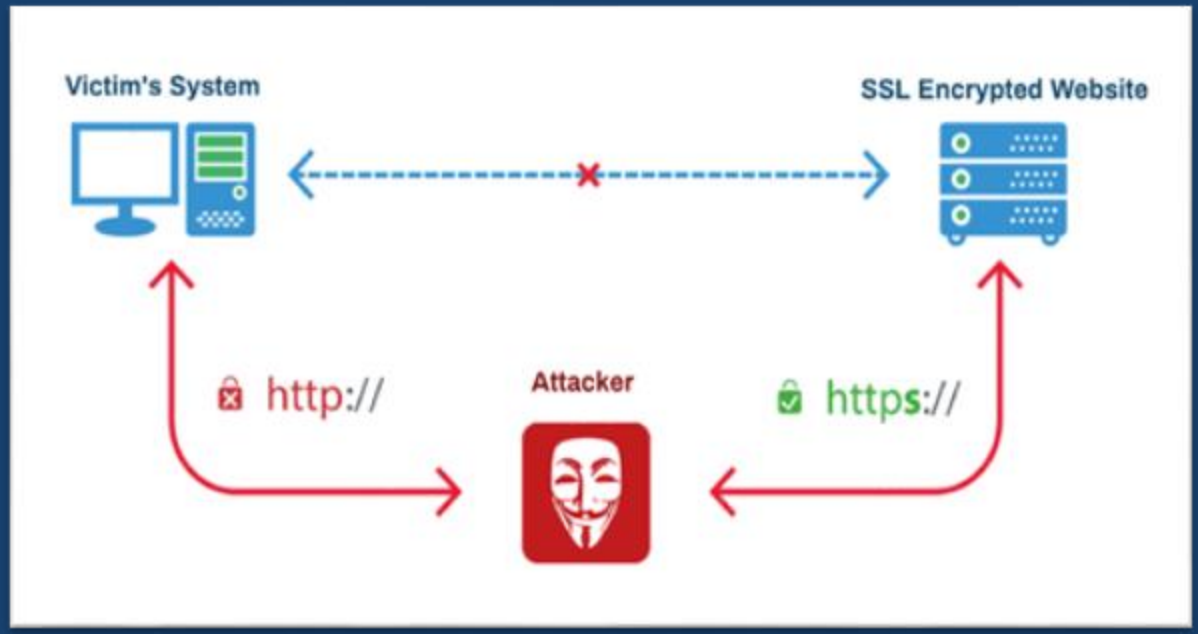
Client/server

Client/server

Phishing Attack



- : Example Attacks on social media: Fake likes, Fake plugins, fake offering

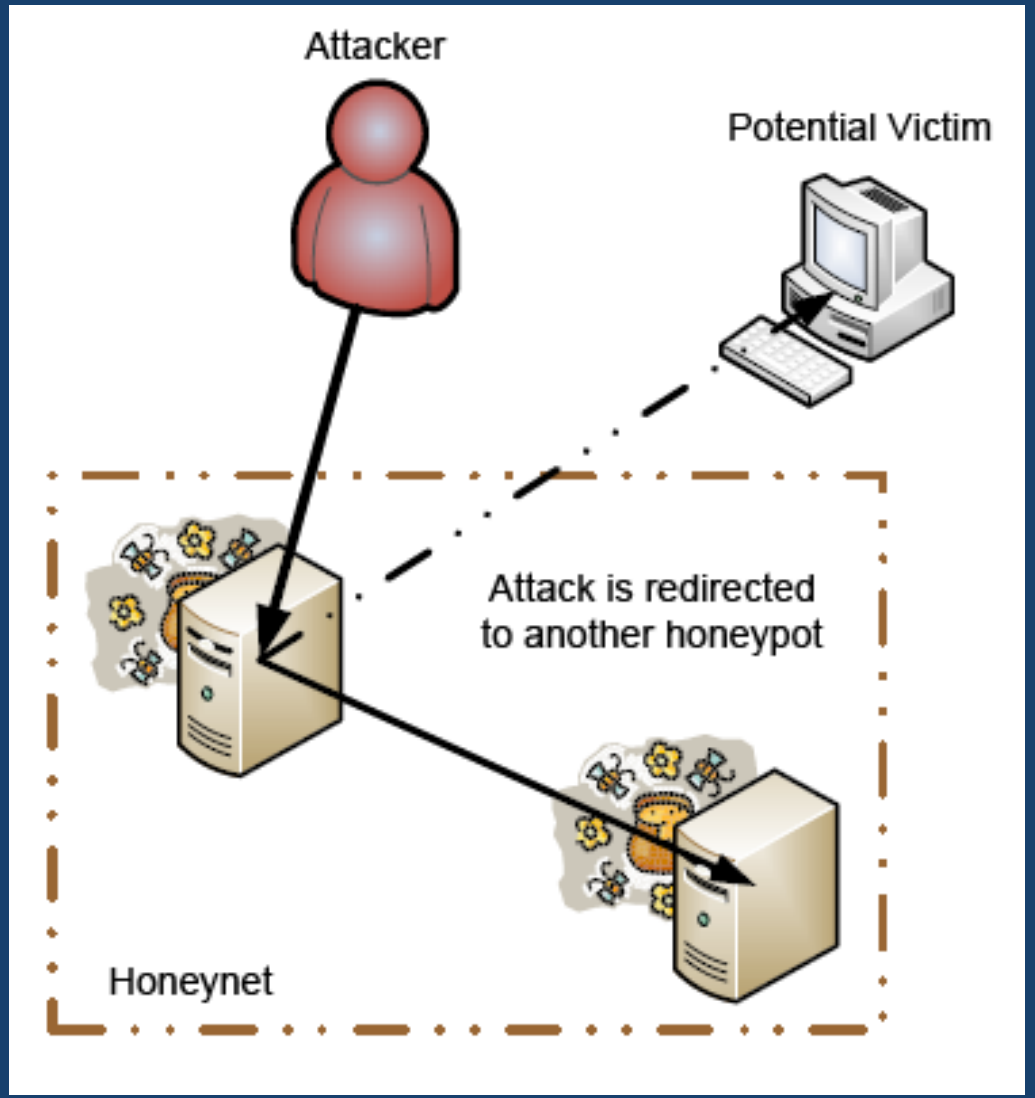


HONEY POT

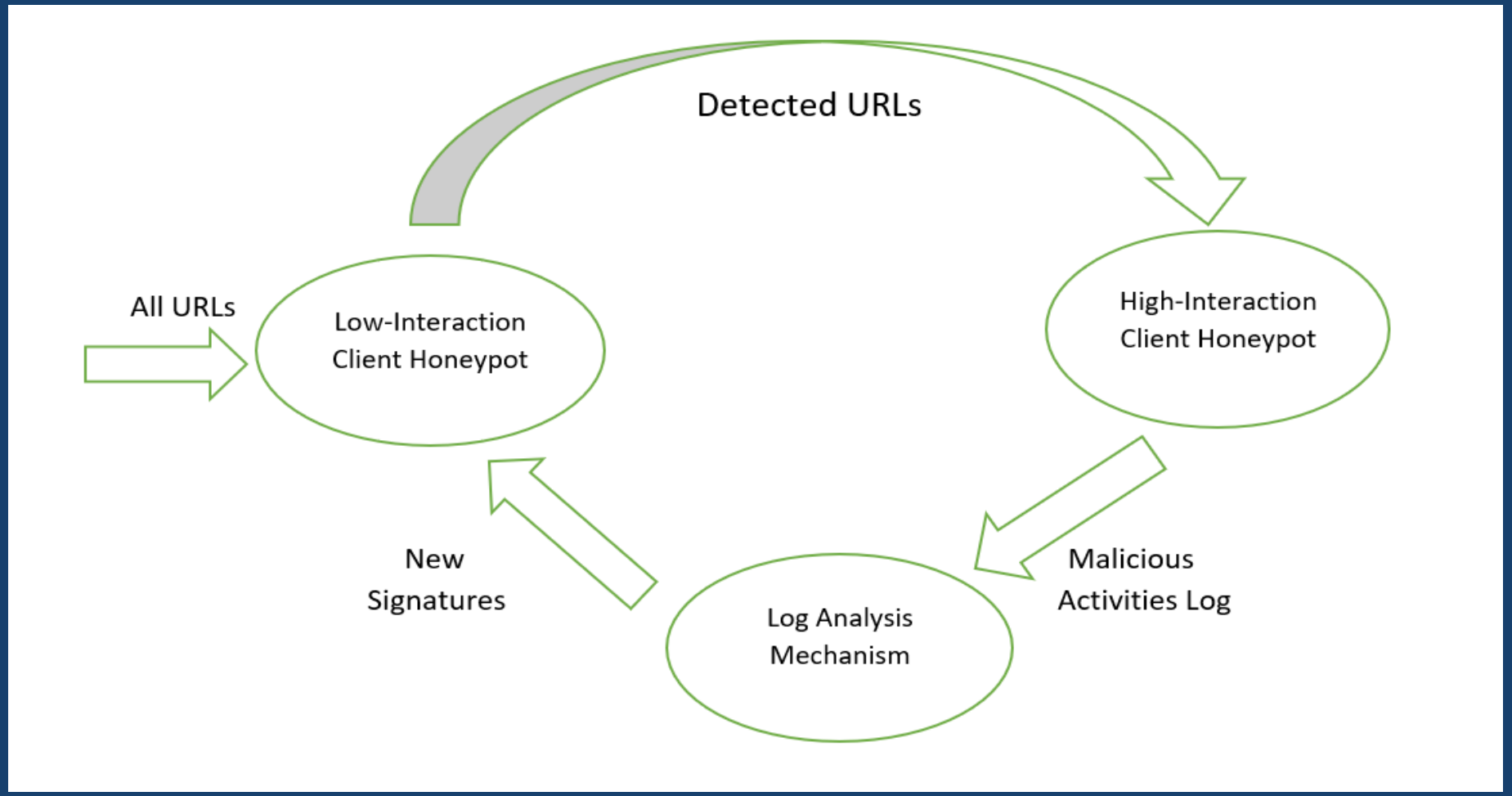
Existing methods to prevent this kind of attacks is the use of honeypots but they still have some loopholes/vulnerabilities which attackers take advantage of.

Examples of tool hackers use to detect a honeypot in the network (Shodan, n-map, etc.).

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



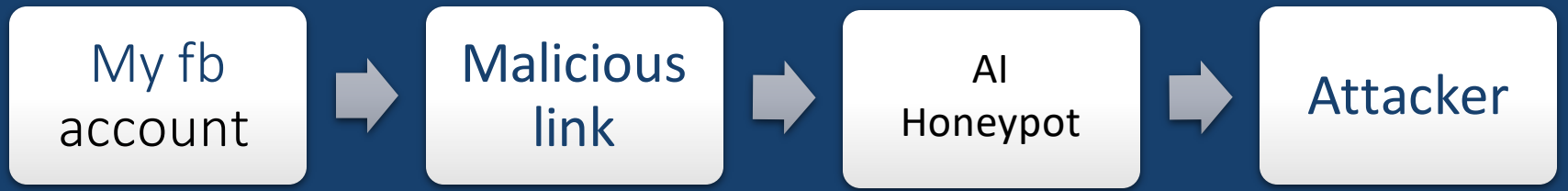
Our Analysis Model of Honey pot using AI



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 :

OUR IMPLEMENTATION:



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 and do heuristic analysis to detect any part of malicious code.

1st level : Low Interaction Client Honey pot

Heuristic Analysis

Heuristics refers to a set of rules as opposed to a specific set of program instructions used to detect malicious behaviour without having to uniquely identify the program responsible for it (used in traditional methods).

All URLs confront the Low Interaction Client Honeypot in the beginning where heuristic analysis is used to detect the malicious part of the code in the link by reading the source code.

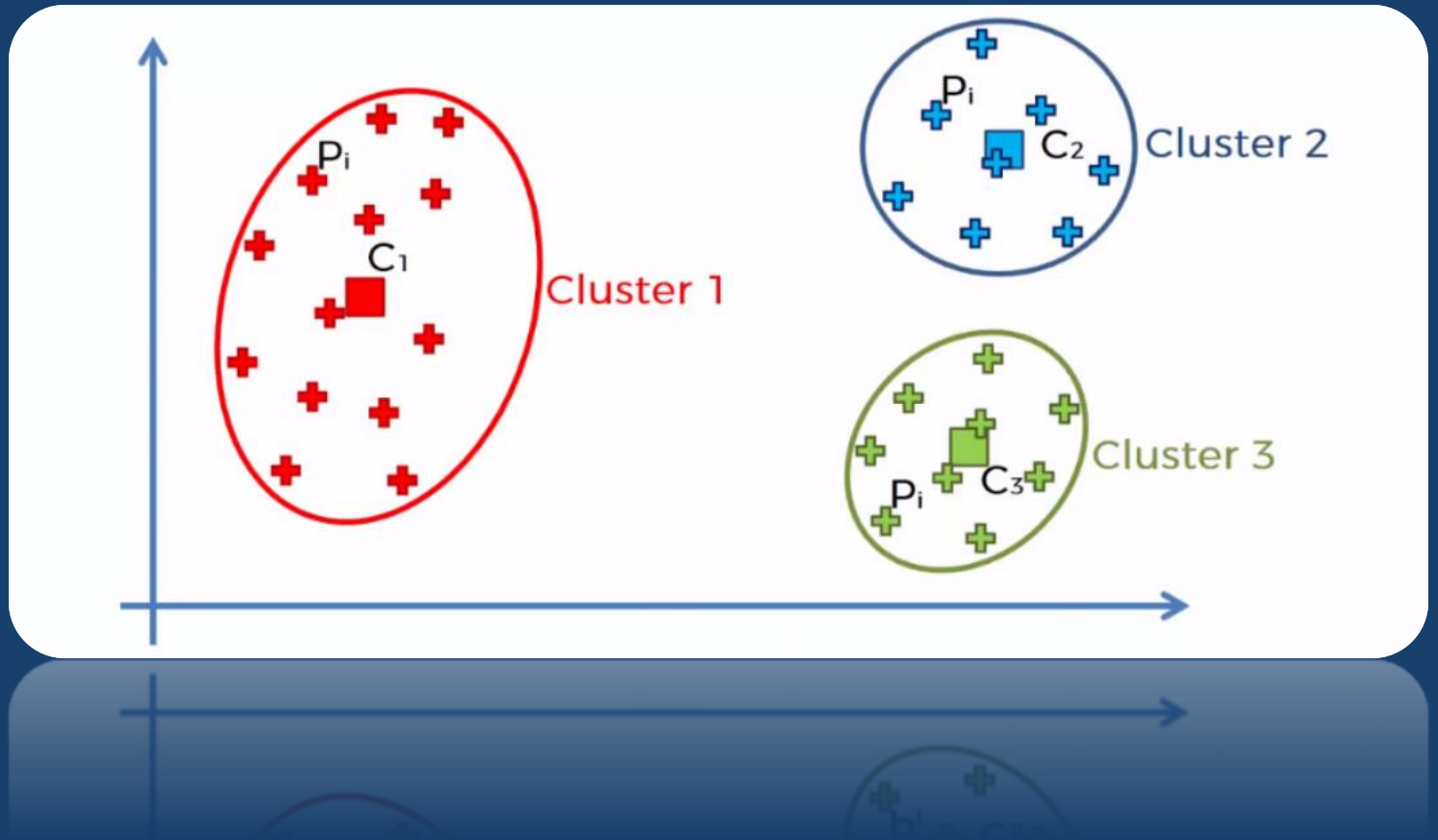
The heuristic engine used by an antimalware program include rules for the following:

- a program which tries to copy itself into other programs (in other words, a classic computer virus)
- a program which tries to write directly to the disk
- a program which tries to remain resident in memory after it has finished executing
- a program which decrypts itself when run (a method often used by malware to avoid signature scanners)
- a program which binds to a TCP/IP port and listens for instructions over a network connection (this is pretty much what a bot—also sometimes called drones or zombies—do)
- a program which attempts to manipulate (copy, delete, modify, rename, replace and so forth) files which are required by the operating system
- a program which is similar to programs already known to be malicious

2nd level : High Interaction Honey pot

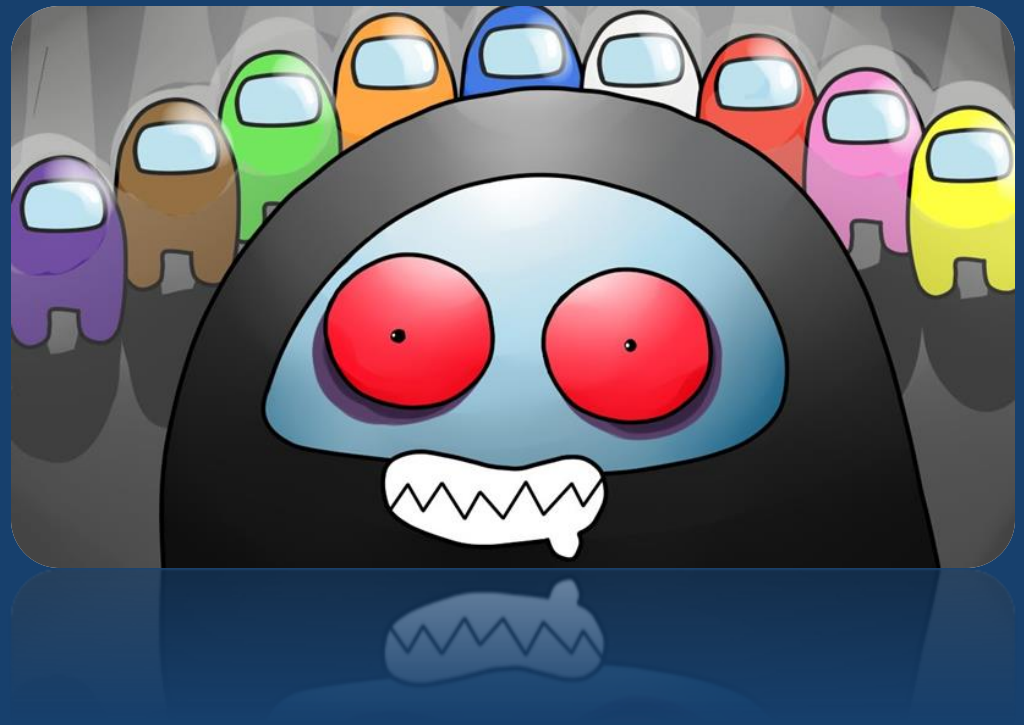
Instead of redirecting it to the fake server, the link is forwarded to the high interaction honeypot to identify the type of malicious code/script is used.

Working of high interaction honeypot:
Log files(For e.g. Capture tool) 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.



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!