MALWARE CAPTURING HONEYPOT : DIONAEA

Sarosh Petkar | Prof. Jonathan Weissman | RIT

PROBLEM STATEMENT

The Internet can be a dark and dangerous place; featuring a variety of malware such as worms, viruses and Trojan horses that are aimed at conducting cyber-attacks and as result stealing personal information such as usernames and passwords. Thus, proliferation of malware poses a significant threat to modern computer technologies.

Conventional systems like AV, IDS and IPS rely heavily on known malicious signatures to detect malicious traffic and hence these systems have been at a serious disadvantage when it comes to detecting never before seen polymorphic and metamorphic malware.

PROJECT OVERVIEW

The aim of the project is to collect malware using a honeypot in order to understand what is trending in the dark malware underworld. All the malware communication would be tracked and displayed through the use of a geolocation based visualization module.

WHAT IS A HONEYPOT

A honeypot is a decoy security resource that is designed to draw attacks as a means of detection, deflection and information gathering. The strategy behind this reconnaissance tool is to obtain intelligence by monitoring and logging every action.

DIONAEA

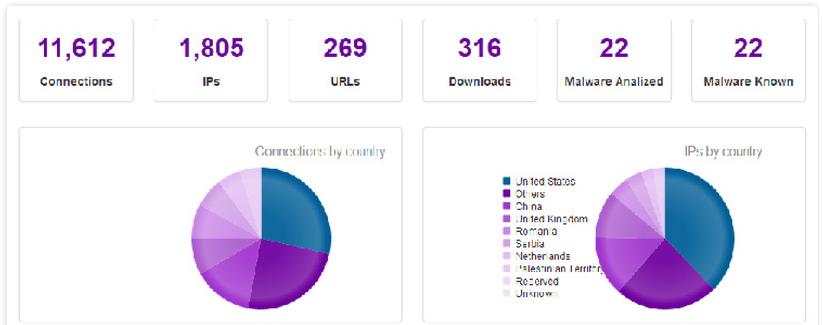
Dionaea is named after the genus of plants that includes the Venus flytrap. The symbolism is apparent.
Dionaea is a low-interaction python-based honeypot that emulates a vulnerable Windows system in an effort to capture malware samples or interaction from malicious entities.

- Dionaea sends real-time notification of attacks via XMPP and logs the information into a SQLite database.
- It uses Libemu to detect and capture shellcode.

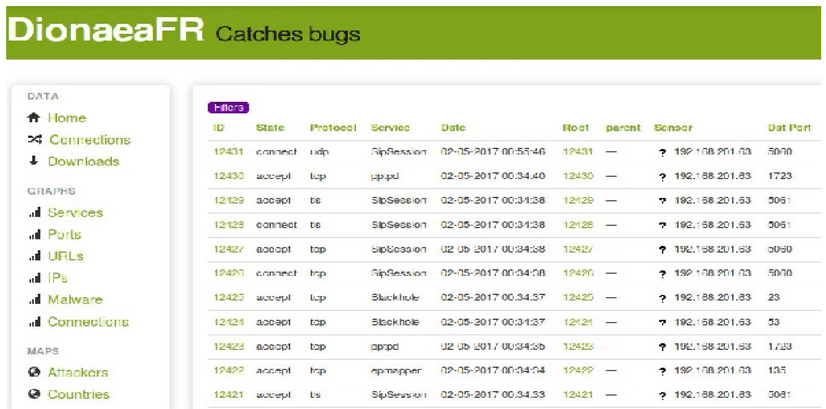
R·I·T COMPUTING SECURITY

RESULTS

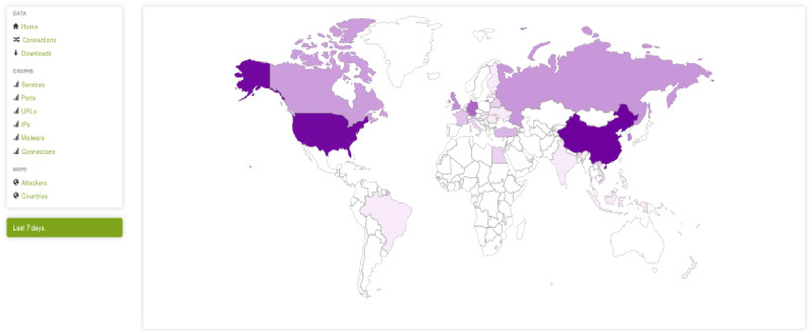
Interface:



Connections:



Attacker Map:



MALWARE

URL	MD5	Classification
txxp://46.128.183.60/host.exe	fd1fb45d7ca1eeef06f5d46a3e9a3d2f	Backdoor
txxp://46.128.172.44/host.exe	47b2e95136e66052206722 1ae405025c	Worm
hxxp://87.20.127.177/Photo.scr	ABA2D86ED17F587EB6D5 7E6C75F64F05	Trojan
hxxp://158.255.6.208/task3.exe	841867D08E7D92E1FB633 C61AB421D53	Trojan
hxxp://hibiscus.com.my/g2n-x688-esp/	F8AD349FF58F24D1DDF39 F468822B510	Trojan

- The honeypot collected 55 different samples as distinguished by the MD5 hashes. Of these 22 were identified as malware by Virustotal.
- Of the known samples, many were Trojans such as GenericKD, WisdomEyes and CoinMiner.
- The rest were variants of bot families like Spybot, Polybot and others. The majority of binaries, had some kind of IRC backdoor functionality.

CONCLUSION

One of the key mottos within information security is, “Prevention is ideal, but detection is a must.” We must realize that an organization’s key resources will be attacked, and we have to be ready to detect the attack as early as possible. However, it is imperative to understand that a Honeypot does not replace existing security technologies but works alongside them by monitoring activity occurring on the system.

FUTURE WORK

- Incorporate pro-active and re-active defensive techniques like blacklisting and dynamic quarantine.

- Generation of phylogeny models, using techniques similar to those used in bioinformatics, may help to reconcile naming inconsistencies and assist in the investigation of new malicious programs. Additionally, advanced techniques such as generic decryption scanning and negative heuristic analysis are required for detection.

REFERENCES

- https://www.edgis-security.org/honeypot/dionaea/
- https://github.com/rubenespadas/DionaeaFR