UNIVERSITY *of* NICOSIA

HoneyCY: An Active Defense Framework

Dr Harald Gjermundrød

University of Nicosia

Talk Outline

- Active Defense Concept
- Active Deception - Honeypot
- HoneyCY Framework

Cyber Warfare is a Reality!

NEWS

Cyberspace is officially a war zone – NATO

By *Catherine Hardy*

Follow @fernojay

15/06 10:23 CET | updated at 15/06 - 18:27

A A

Cyberspace is the new front in global war – according to NATO.

The declaration was made after a meeting of defence ministers from the organisation's member nations.

"We agreed that we will recognise cyberspace as an operational domain, just like air, sea and land"

Making cyberspace an official war zone means attacks carried out in this context could trigger an Article 5 response.

collective action by the 28-member organization against the perpetrator of an incident aimed at any NATO-protected state.

Let’s Think Outside the Box!

The Case of Active Defense

This is an invited essay by the 2013 IFIP TC-11 Kristian Beckman Award recipient

Framework and principles for active cyber defense☆

*Dorothy E. Denning**

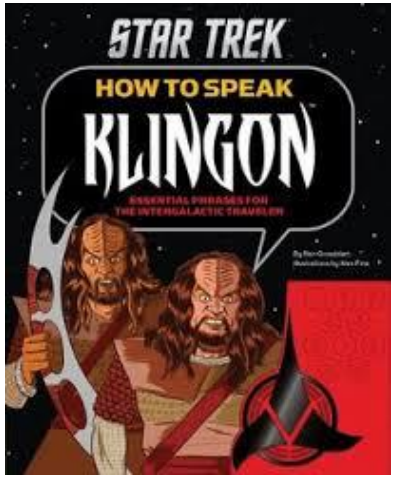
Naval Postgr aduate School, Monterey, USA

- Not Hacking Back!
- Active and Passive Air Defense applied to cyber domain
- Active defenses are direct actions taken against specific threats, passive defenses focus more on making cyber assets more resilient to attack

Talk Outline

- Active Defense Concept
- Active Deception - Honeypot
- HoneyCY Framework

Active Deception - Honeypot



Study the attackers!

Profile the attackers!

Profile the attacks!

Active Deception – Honeypot [2]

Set a trap to lure attackers and study their attack patterns

Additional intelligence can be gathered on the attackers' capabilities

Honeypot Essentials - Definition

No consensus on the definition!

For our purposes, a honeypot is a security resource whose value lies in being probed, attacked, or compromised.

GOAL:

- having it being probed and/or exploited due to the deliberate planting of vulnerabilities
- analyze the compromised system
- gain knowledge about the nature of the attack and the attacker patterns.

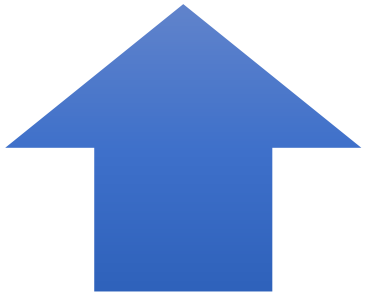
Talk Outline

- Active Defense Concept
- Active Deception - Honeypot
- HoneyCY Framework

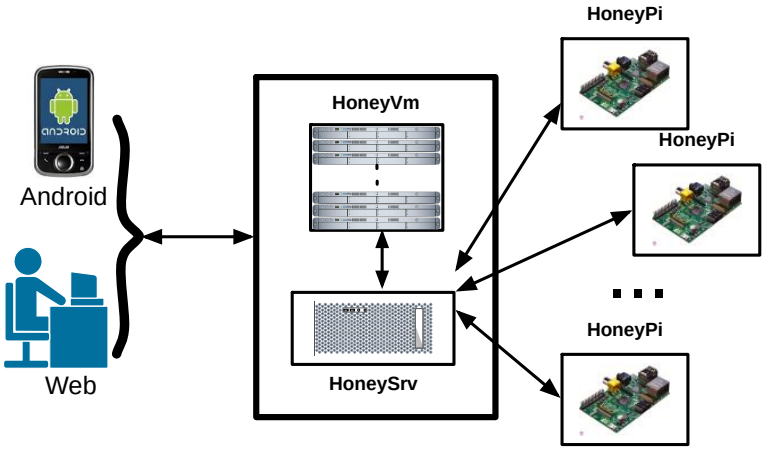
Need for HoneyCY☺

Deployment and configuration of many available open-source honeypots is nontrivial due to either inadequate (or outdated) documentation or overall complexity. Often, there is lack of visualization of the attack details.

Wrap and integrate a set of complimentary honeypot solutions in an easy and cost-effective deployment package that offers visualization of the collected information.



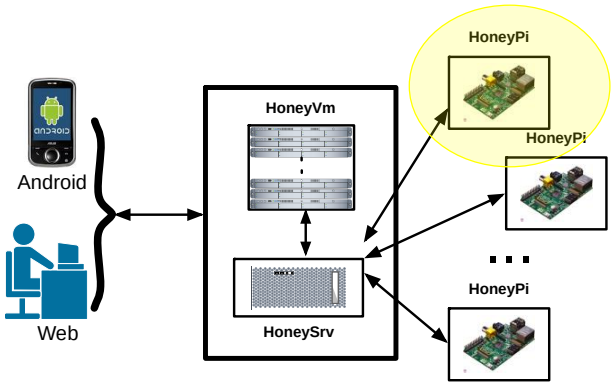
HoneyCY – High Level Architecture



3-tier architecture

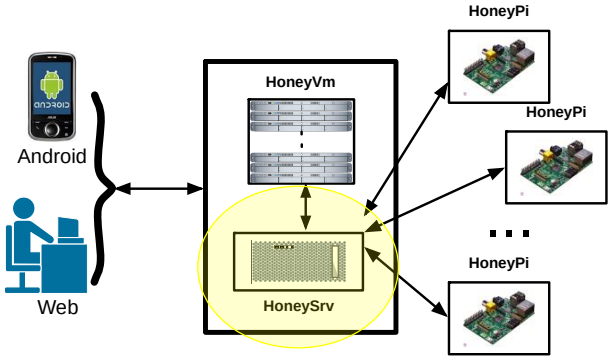
The complete system provides for distributed “sensors” for capturing the attacks (**honeyPi**), storing the relevant evidence (**honeySvr**), and finally performing post-mortem analysis of collected events to determine the attack vector(s) (**honeyVM**)

HoneyCY – A Typical Interaction Flow



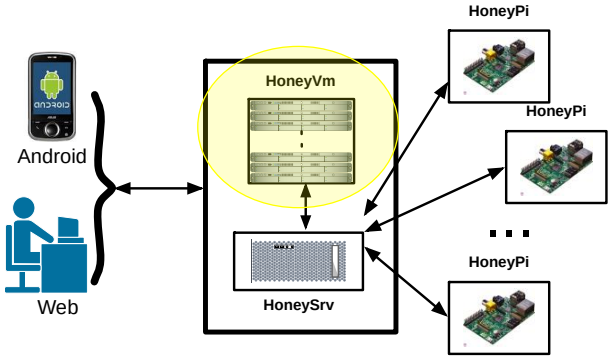
1. honeyPis is experiencing a malware attack (one of the open-source honeypots, configured to run inside the specific honeyPi, captures the attack attempt and stores the uploaded malware)

HoneyCY – A Typical Interaction Flow [2]



2. During honeySrv's next event collection iteration, the captured malware gets transferred to the honeySrv server. The collection procedure is executed automatically every 30 minutes (this is configurable and another interval can be selected). Analysis takes place here for known malware and appropriate action is taken.

HoneyCY – A Typical Interaction Flow [3]



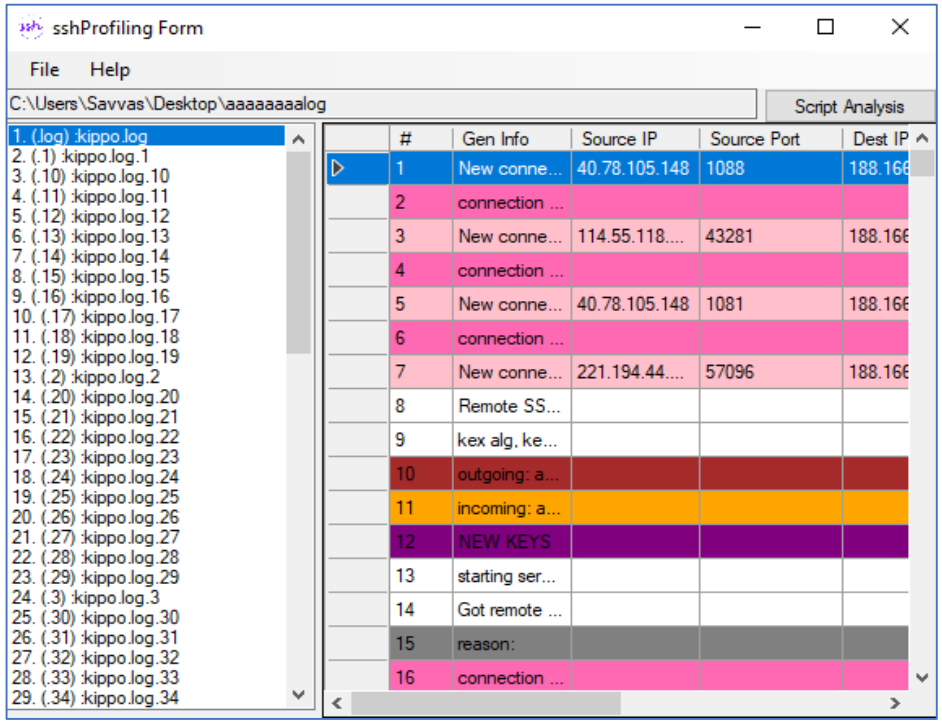
3. In the case the automatic analysis concludes that the collected malware is a new one, it is sent to the honeyVM where the malware is executed within a sandbox with the intention to discover the attack pattern.

HoneyCY Deployment

- **24h experiment** - HoneyCY reported an overall number of 188 attacks during the testing period of 24 hours.
  - 108 attacks were launched from a single IP (not able to determine its location), followed by 47 attacks attacks originating from an IP in the USA.
  - The most probed ports were ports 80 (114 attacks), 1433 (54 attacks), and 443 (15 attacks).
  - Alerts were emailed to the system administrator as attacks were happening.
- **365d experiment** - An astonishing number of 35174 connections probed the honeypot services
  - Originating from 783 unique IPs, capturing a total of 12486 files.
  - The most commonly attacked port was port 445, followed by ports 3306, 1433 and 8000 (used by Apache).
  - More than half of the attacks originated from Hungary, followed by Germany and Brazil.
  - Many captured malware were investigated in more detail using Dionaea's EMU plugin.

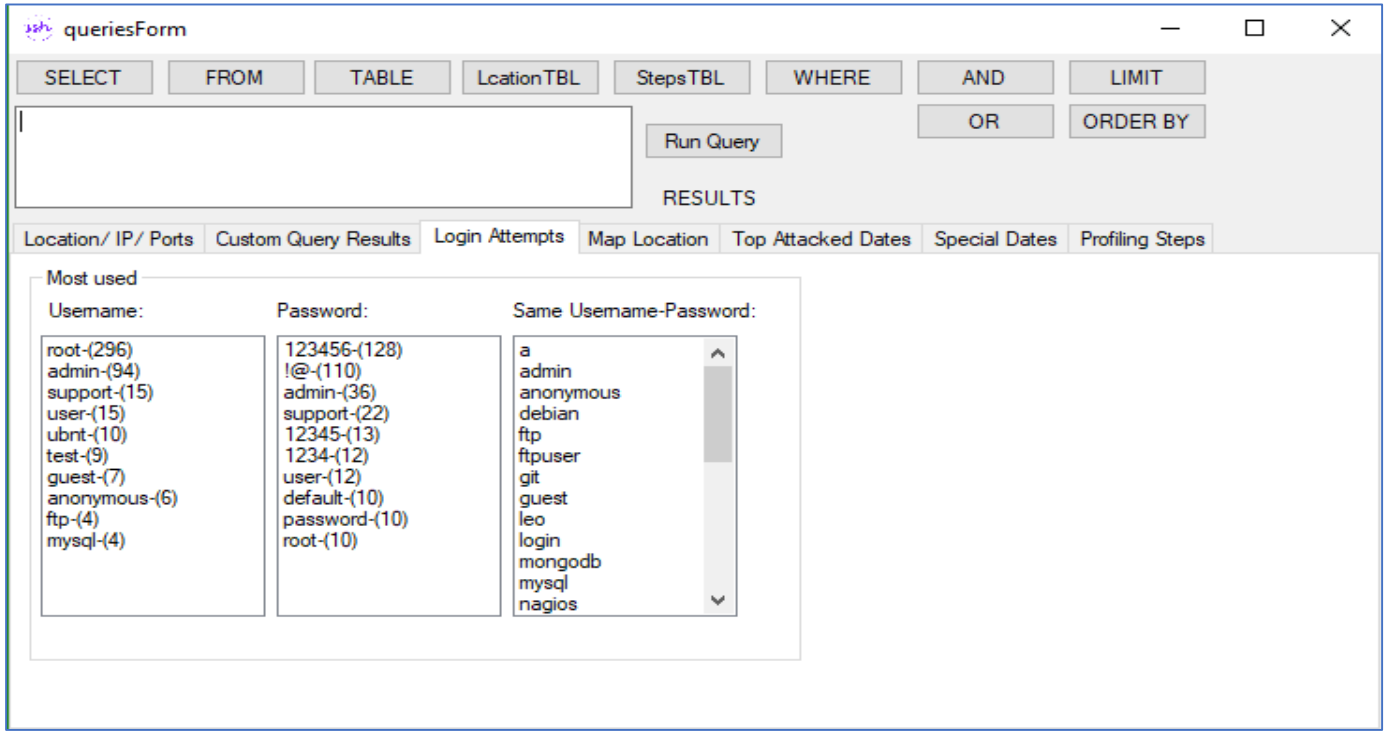
Profiling and Analyzing Tool

- Tool to assist in investigation of the obtained results

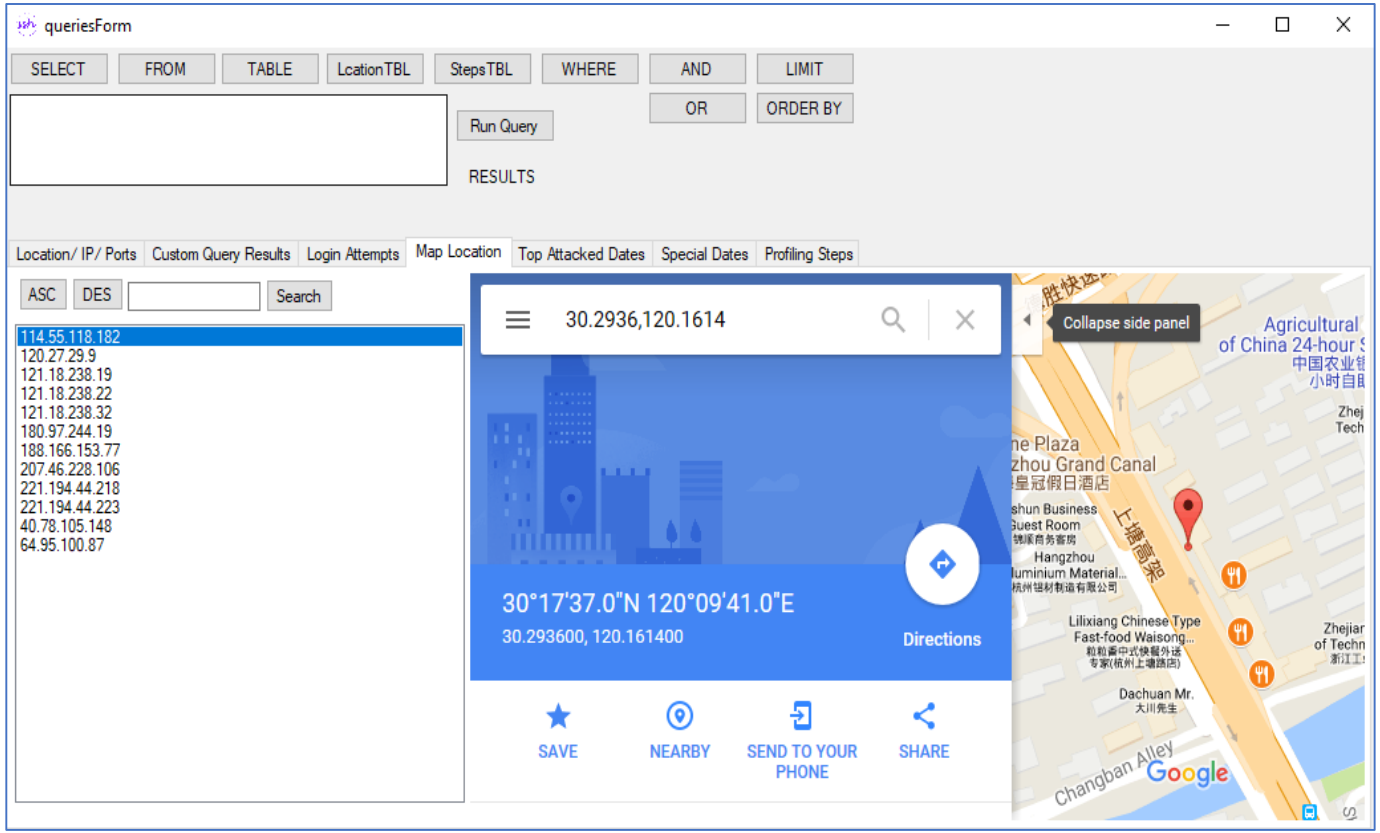


Profiling and Analyzing Tool [2]

- Provides query facility to search for patterns (profiling)

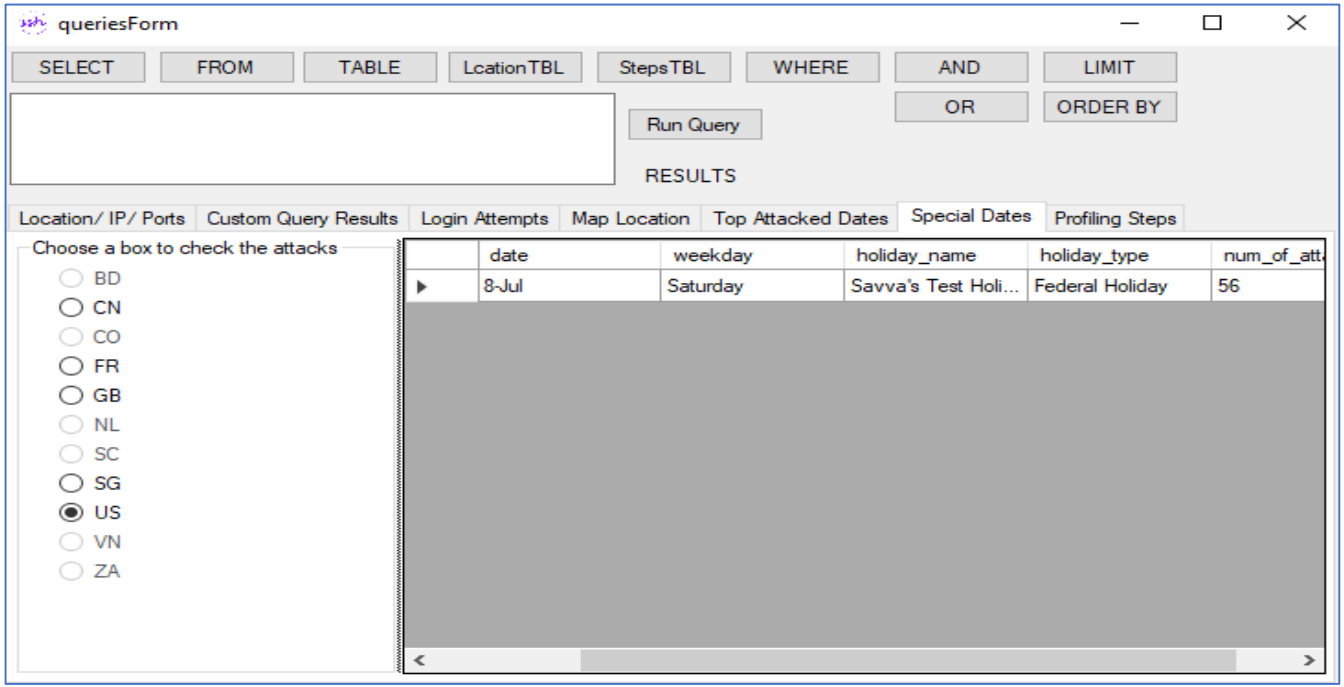


Profiling and Analyzing Tool [3]



Profiling and Analyzing Tool [4]

- Does the attacker work on public holidays/weekends/after hours?
  - i.e. is the attacker an employee somewhere?



Summarizing

Cyberattacks are becoming the greatest threats to complex network environments

- Resort to unconventional non-traditional security mechanisms
- Utilize honeypots that lure attackers to probe the hosted services in order to profile their attack behavior

HoneyCY

- a comprehensive open-source system that integrates mature honeypot implementations into a single inexpensive framework that is easy to deploy, configure, and has provision for visualization, profiling, and other management support.

Thanks for your attention!

For more info, contact me at gjermundrod.h@unic.ac.cy

Thanks to the honeyCY members of the Informatics Security Laboratory

http://isl.unic.ac.cy

Dr Ioanna Dionysiou (Co-Director), Andreas Christoforou, Panayiotis Toumpas, Savvas Karasavvas