



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 @fermojey

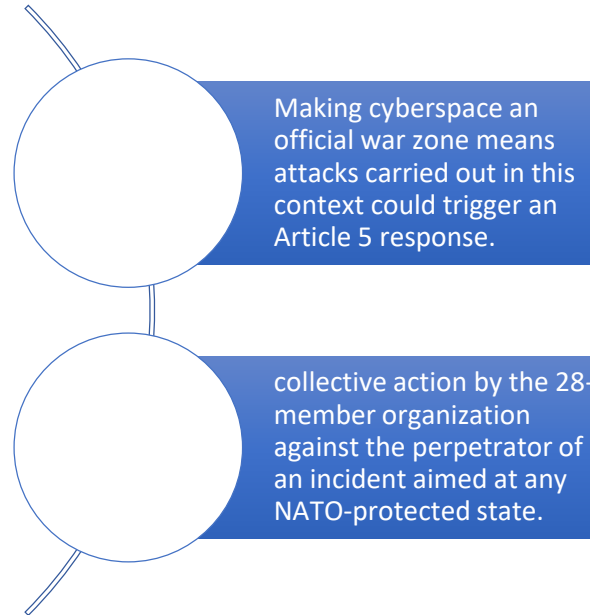
15/06 10:23 CET | updated at 15/06 - 18:27



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"



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 Postgraduate School, Monterey, USA



Not Hacking Back!

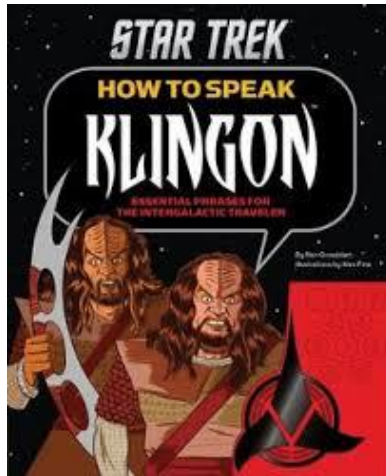
Active and Passive Air Defense applied to cyber domain

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



Honey-pot 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[☺]

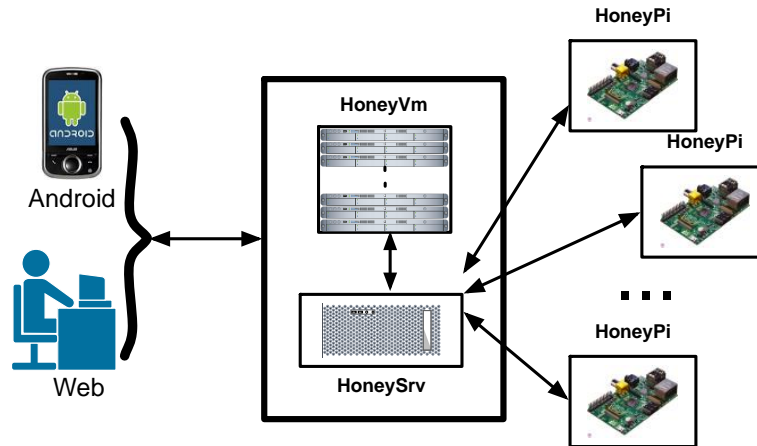


Deployment and configuration of many available open-source honeypots is nontrivial due to either inadequate (or outdated) documentation or overall complexity. Often, there is lack of visualization of the attack details.

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



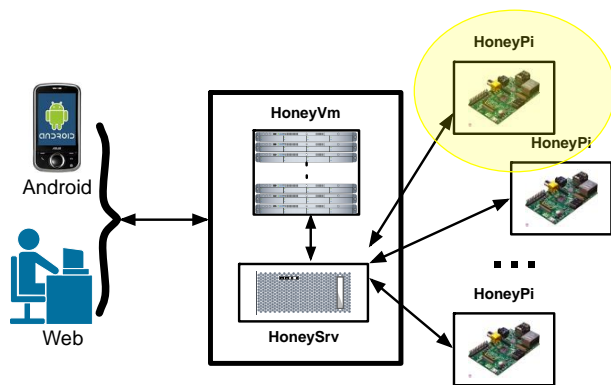
HoneyCY – High Level Architecture



3-tier architecture

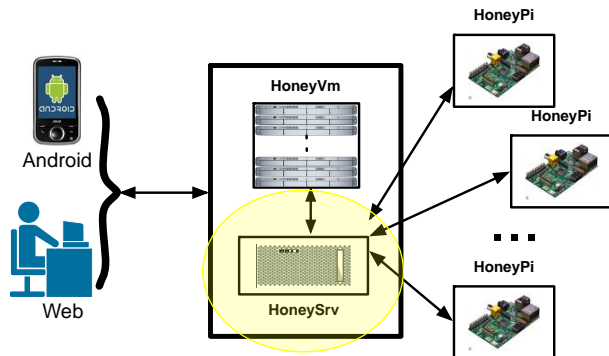
The complete system provides for distributed “sensors” for capturing the attacks (**honeyPi**), storing the relevant evidence (**honeySvr**), and finally performing post-mortem analysis of collected events to determine the attack vector(s) (**honeyVM**)

HoneyCY – A Typical Interaction Flow



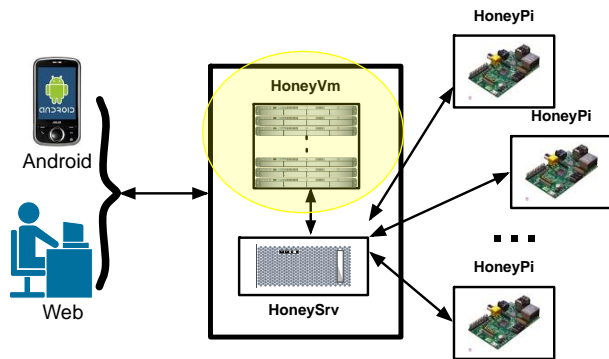
1. honeyPis is experiencing a malware attack (one of the open-source honeypots, configured to run inside the specific honeyPi, captures the attack attempt and stores the uploaded malware)

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]



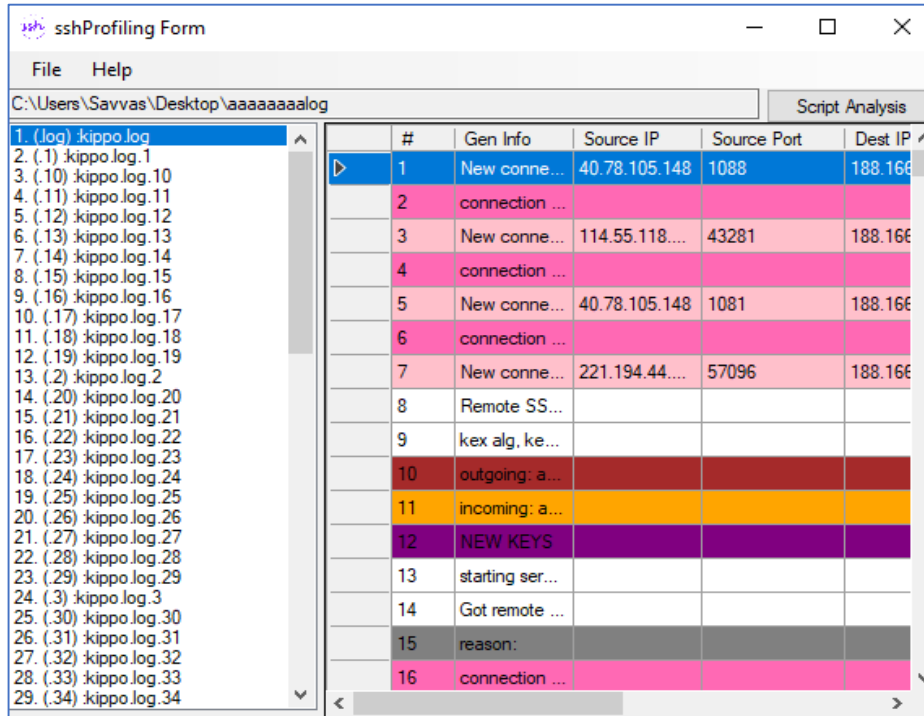
3. In the case the automatic analysis concludes that the collected malware is a new one, it is sent to the honeyVM where the malware is executed within a sandbox with the intention to discover the attack pattern.

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 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



The screenshot shows the 'sshProfiling Form' application window. The title bar includes the application name and standard window controls. The menu bar contains 'File' and 'Help'. The address bar shows the file path 'C:\Users\Savvas\Desktop\aaaaaaaaalog' and a 'Script Analysis' button. The left pane displays a list of log files from '1. (.log) kippo.log' to '29. (.34) kippo.log.34'. The right pane is a table with the following data:

#	Gen Info	Source IP	Source Port	Dest IP
1	New conne...	40.78.105.148	1088	188.166
2	connection ...			
3	New conne...	114.55.118...	43281	188.166
4	connection ...			
5	New conne...	40.78.105.148	1081	188.166
6	connection ...			
7	New conne...	221.194.44....	57096	188.166
8	Remote SS...			
9	kex alg, ke...			
10	outgoing: a...			
11	incoming: a...			
12	NEW KEYS			
13	starting ser...			
14	Got remote ...			
15	reason:			
16	connection ...			

Profiling and Analyzing Tool [2]

- Provides query facility to search for patterns (profiling)

The screenshot shows a web-based application window titled "queriesForm". At the top, there is a query builder interface with buttons for "SELECT", "FROM", "TABLE", "LocationTBL", "StepsTBL", "WHERE", "AND", "LIMIT", "OR", and "ORDER BY". A "Run Query" button is located to the right of a text input field. Below the query builder, there is a "RESULTS" section with a tabbed interface. The active tab is "Login Attempts". The results are displayed in a table with three columns: "Username:", "Password:", and "Same Username-Password:". The table contains the following data:

Username:	Password:	Same Username-Password:
root-(296)	123456-(128)	a
admin-(94)	!@-(110)	admin
support-(15)	admin-(36)	anonymous
user-(15)	support-(22)	debian
ubnt-(10)	12345-(13)	ftp
test-(9)	1234-(12)	ftpuer
guest-(7)	user-(12)	git
anonymous-(6)	default-(10)	guest
ftp-(4)	password-(10)	leo
mysql-(4)	root-(10)	login
		mongodb
		mysql
		nagios

Profiling and Analyzing Tool [3]

The screenshot displays the 'queriesForm' application interface. At the top, there is a query builder with buttons for 'SELECT', 'FROM', 'TABLE', 'LocationTBL', 'StepsTBL', 'WHERE', 'AND', 'LIMIT', 'OR', and 'ORDER BY'. A 'Run Query' button is positioned to the right of a large text input field. Below the query builder, there are tabs for 'Location/ IP/ Ports', 'Custom Query Results', 'Login Attempts', 'Map Location', 'Top Attacked Dates', 'Special Dates', and 'Profiling Steps'. The 'Map Location' tab is active, showing a list of IP addresses on the left and a Google Maps view on the right. The IP list includes: 114.55.118.182, 120.27.29.9, 121.18.238.19, 121.18.238.22, 121.18.238.32, 180.97.244.19, 188.166.153.77, 207.46.228.106, 221.194.44.218, 221.194.44.223, 40.78.105.148, and 64.95.100.87. The Google Maps view shows a location in Hangzhou, China, with coordinates 30°17'37.0"N 120°09'41.0"E and address 30.293600, 120.161400. The map includes labels for 'Agricultural of China 24-hour', 'Zhejiang Tech', 'Hangzhou Grand Canal', 'Hangzhou Business Guest Room', 'Lilixiang Chinese Type Fast-food Waisong...', 'Dachuan Mr.', and 'Changban Alley'. The Google logo is visible in the bottom right corner of the map.

Profiling and Analyzing Tool [4]

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

The screenshot shows a web-based application window titled "queriesForm". The interface includes a query builder with buttons for "SELECT", "FROM", "TABLE", "LocationTBL", "StepsTBL", "WHERE", "AND", "LIMIT", "OR", and "ORDER BY". A "Run Query" button is positioned below the query input field. The "RESULTS" section is active, displaying a table with the following data:

	date	weekday	holiday_name	holiday_type	num_of_att
▶	8-Jul	Saturday	Savva's Test Holi...	Federal Holiday	56

On the left side of the results area, there is a section titled "Choose a box to check the attacks" with a list of radio buttons for different countries: BD, CN, CO, FR, GB, NL, SC, SG, **US** (selected), VN, and ZA.

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*