14/12/2020

Modern Honey Network Analysis Report

By

Michal Slomski

Contents

1 Introduction

Modern Honey Network (MHN) is an open-source software designed to simplify the deployment of Honeypots. Honeypots are fake production machines which are compiled with intentionally vulnerable software and features which can be exploited. These honeypots are placed inside or outside a network with a desired purpose.

Mercolino (2015) mentions several desired goals for the use of MHN as:

- One of the goals is to deploy a fake server, where the attacker could waste time performing attacks. This time is used by the system administrator to block the attacker and secure the rest of the real production servers
- Another goal is to learn the techniques used by the attackers to gain and exploit the services.
- Some honeypots are capable to capture malware, exploits, etc… that helps to catch zero-day attacks and to reverse engineer them to create the protection.
- The honeypots used internally on your network could help you to catch security breaches that are using your platform to launch other attacks. (Mercolino, 2015)

The modern honey network is an excellent tool to defend business resources and networks from attackers. However, they are also capable of causing a significant amount of damage to the network or business if managed or deployed incorrectly. This is due to attracting more potential attackers as they are designed to be exploited. This can lead to exploitation of the network and data contained on the network. If the honeypots are used correctly, they can be utilized as decoys to distract the attackers from actual information.

According to Mercolino (2015), “The honeypots could be a double edge tool, because if they are not used correctly could be attract more attacks to your network and if the server is compromised for any reason then your network could be vulnerable to other attacks.”

1.1 Types of Honeypots

There are different types of honeypots available to deploy in the Modern Honey Network. This can be achieved from the MHN console by simply selecting a honeypot, copying, and executing the deployment script. The different types of honeypots are divided into three categories:

- Low Interaction
- High Interaction
- Sticky Honeypots

Low interaction honeypots emulate services which are considered the most common to exploit. However, these services cannot be exploited, hence the name low interaction. The advantage to these honeypots is that they are very simple to maintain and deploy.

The second type, high interaction honeypots, emulate real services which are fully exploitable. The disadvantage to these honeypots is their deployment difficulty and high maintenance requirement. Successful exploits may also lead to new attack vectors against real systems.

Sticky honeypots, also known as tarpits, are virtual machines generated using available IP addresses which are unused. These virtual machines emulate real services creating a much larger field for an attack. The advantage of this honeypot is that due to its number of exploitable services, it can keep an attacker occupied for much longer.

1.2 Software Information

The Modern Honey Network used in this analysis report was hosted on a droplet (VM) provided by DigitalOcean (linked in Annex A). There are four droplets running, with each one hosting at least one sensor. There are ten active sensors (Honeypots) hosted on the MHN.

Two types of honeypots are deployed, Kippo (Cowrie) and Conpot. These honeypots were gathering data for at least a month for analysis. The details of the honeypots and data analysis can be found in section 2 and 3.

2 Research

2.1 Kippo

Kippo, also known as Cowrie, is a medium interaction type of honeypot. It is designed to capture SSH brute force attacks. It is also capable of capturing the entire shell interaction between the honeypot and the attacker.

Honeynet.org (2019) mentions several interesting features of the Kippo honeypot as:

- Fake filesystem with the ability to add and remove files. A full fake filesystem resembling a Debian 5.0 installation is included
- Possibility of adding fake file contents so the attacker can 'cat' files such as /etc/passwd. Only minimal file contents are included
- Session logs stored in an UML Compatible format for easy replay with original timings
- SSH emulates connections, pretending to execute actions which do not serve a purpose

2.2 Conpot

Conpot is a low interaction honeypot designed for server-side Industrial Control Systems. It is very simple to deploy and maintain. By providing a range of industrial control protocols, this honeypot is capable of emulating large and complex infrastructures. This can fool an attacker to thinking that they have found an industrial infrastructure.

The deceptive capabilities were improved when a possibility to server a custom human machine interface was added. This greatly increases the honeypots' attack surface. Honeypot.org (2019) says "the response times of the services can be artificially delayed to mimic the behaviour of a system under constant load."

This honeypot can be accessed through productive HMI's or extended with real hardware, provided with a complete stack of protocols.

3 Data Analysis

The data was analysed using the Splunk console. This was integrated within the Modern Honey Network hosted. The MHN was configured to generate a log file in a Splunk readable format. The Splunk console provides a very convenient and simple to navigate user interface. All live data generated is immediately parsed to the console, ready to view and analyse.

3.1 Kippo

As mentioned in the previous section, Kippo is an SSH logger which captures brute force attacks and SSH activity. Therefore, majority of valuable collected data by this honeypot are SSH usernames and passwords. There is a total of five Kippo honeypots deployed.

The Splunk console can sort the data into categories such as top passwords and top username/password combinations. The results are displayed in the tables on the dashboard. These results can be found in the table 1 and 2 below.

Table 1 – Top SSH Passwords

ssh_password	count
123456	909
nproc	676
123	452
admin	393
user	379
password	286
test	237
1234	187
support	183
raspberry	148

Table 2 – Top Username/Password Combinations

ssh_username	ssh_password	count
nproc	nproc	676

user	user	363
admin	admin	329
test	test	207
support	support	182
pi	pi	146
ubnt	ubnt	134
postgres	postgres	129
ubuntu	ubuntu	128
oracle	oracle	122

All attacks appear to be launched against the port 22. This is due to the settings in the honeypots being left at default before launch. This could be changed or expanded in the future.

The main MHN console is very useful for analysing Kippo results. On the main page, the previous results can be seen. However, an additional list called 'Top 5 Attacker IP addresses' is displayed. The list shows each attacker's country flag as well as the IP address. The results from this list are shown in table 3.

Table 3 – Top 5 Attackers

Country	IP Address	Count
Panama	**45.227.255.163**	**3425**
Ireland	**5.188.86.172**	**2957**
Ireland	**5.188.86.174**	**2182**
Panama	**45.227.255.205**	**1780**
Ireland	**5.188.87.53**	**1090**

The top attacker's IP address appears to be in Panama. A quick search through the results reveals that this attacker only attacked the Kippo honeypot on port 22.

The attackers in position two and three in table 3 appear to have almost identical IP addresses. This is an interesting result as it suggests two attackers working together, connected to the same network. Perhaps one attacker may be using two machines to increase efficiency of scans and exploits. The total

count of their attacks is very similar as well. These are most definitely two sources working together. Upon closer inspection, these attackers also only attacked the Kippo honeypot on port 22.

After navigating back to the Splunk console for further analysis, new details are discovered. When one of the results are selected, a list of events appears. All events messages appear to have the same or similar contents due to all being on the same port. However, they reveal more details about the attacks, which can be found in table 4.

Table 4 – Kippo Attack Details Example

Type	**Content**
Date	14-12-2020
Direction	Inbound
Protocol	IP
Ids_type	Network
Destination	68.183.119.19
Ssh_username	Ftpuser
App	Cowrie
Transport	TCP
Destination_port	22
Source	159.65.122.192
Source_port	46742
Severity	High
Sensor	3f78bc6a-0ca0-11eb-831f-b2e6b8a57885
Ssh_password	123456
Ssh_version	SSH-2.0-libssh2_1.4.3
Type	cowrie.sessions
signature	SSH login attempted on cowrie honeypot

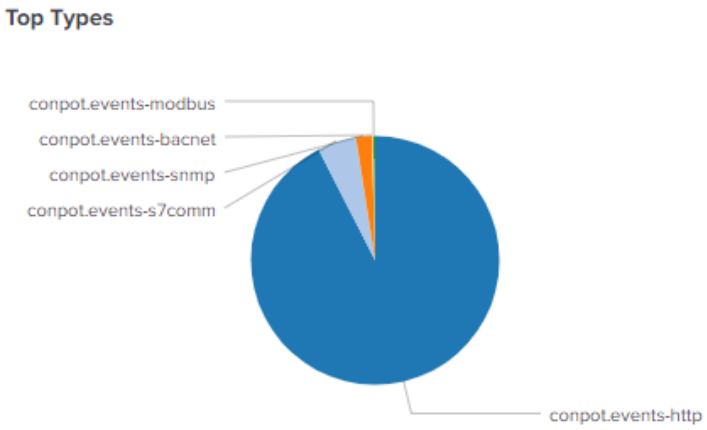
The table contains an example of the most recent attack. All event details for the Kippo honeypot look identical, with altered minor details such as IP addresses, ports, and sensors.

The most valuable details are source ports, source addresses, usernames, and passwords from the incoming exploits. A company in this scenario would use those details to identify and block malicious users. They may also locate the source IP addresses if they are poorly disguised.

3.2 Conpot

It was mentioned in the previous section that the Conpot honeypot emulates multiple services to appear as an industrial complex. These services were emulated on port 502. A total of four Conpots were deployed.

Several services were emulated by the Conpots. The Splunk console displays a pie chart of the top services exploited. The pie chart can be found in the figure below.



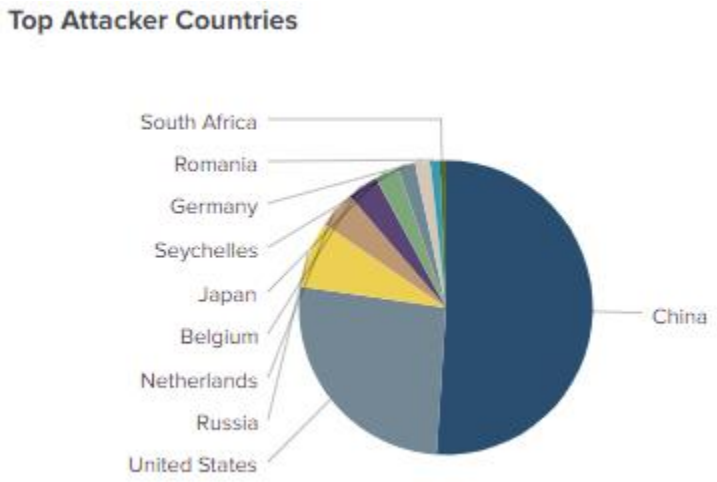
When highlighted, the details of the services are displayed. The values of the details can be found in table 5 below.

Table 5 – Conpot Top Service Types

Service Type	Count	Percentage
Conpot.events-modbus	130	5.76%
Conpot.events-bacnet	21	0.93%
Conpot.events-snmp	93	4.12%
Conpot.events-s7comm	342	15.153%
Conpot.events-http	1671	74.036%

There is a large imbalance of the service types being exploited. It appears that HTTP services are exploited at most part, this is most likely because HTTP services are more common and simpler to exploit than other service types, as HTTP is not secure like HTTPS.

There is a second pie chart displayed in the Splunk console showing the top attacker countries for the Conpot specifically. It is no longer required to verify if the attacker exploited other sensors like with Kippo. The results shown in this section of the console are for Conpots only. The pie chart is shown in the figure below.



When these results are highlighted, the same values are displayed such as count and percentage. From the first glance however, it appears that most attackers responsible for exploiting Conpot honeypot are in China. The details for this pie chart can be found in table 6 below.

Table 6 – Top Conpot Attacker Countries

Country	Count	Percentage
South Africa	14	0.668%
Romania	22	1.049%
Germany	35	1.669%
Seychelles	40	1.907%
Japan	55	2.623%
Belgium	72	3.433%
Netherlands	86	4.101%
Russia	152	7.248%
United States	551	26.276%
China	1070	51.025%

The results for the top attacker countries are quite more divided than the previous results. However, China is exceeding other countries by a large number. The difference between first and second country is large as well, 24.749%.

The Splunk console also shows the top attacker IP addresses just like the MHN dashboard did for Kippo. The results are also filtered for the Conpot, it is no longer necessary to manually verify whether the results are for the specific honeypot only.

The results are shown in a similar format to the results for Kippo in the MHN dashboard. The key difference is that the MHN dashboard only displays top 5 attackers, while the Splunk console displays 10 attackers in the top list. The results from the 'Top Conpot Attackers' list can be found in table 7 below.

Table 7 – Top Conpot Attackers

IP Address	Country	Count
49.74.15.180	China	963
91.241.19.84	Russia	135
84.199.151.106	Belgium	72
51.81.64.17	United States	60
139.162.99.243	Japan	51

195.144.21.56	Seychelles	39
89.248.172.90	Netherlands	18
167.248.133.54	United States	18
162.142.125.40	United States	18
184.154.44.226	United States	17

The attacker that has the highest exploit count on the Conpot honeypot appears to be in China. This may suggest that there is a higher number of malicious users seeking access to an industrial complex specifically. The large difference in the count between first and second attacker proves that majority of attacks were originated in China.

A list of events can be found for Conpot as well. This list shows the details of all exploit events which were registered on the honeypot. One is generated regardless of the service being exploited. All events contain valuable details. However, some values are common in this case as all services share the same port 502. For example, transportation, severity, protocol, ids_type share the same value in each event, regardless of the service type. A full example of the analysed event can be found in table 8.

Table 8 – Conpot Event Details

Type	**Value**
Date	2020-12-14
Time	17:53:31.531728
Source	193.37.255.114
Direction	Inbound
Protocol	IP
Ids_type	Network
Vendor_product	Conpot
Type	Conpot.events-s7comm
Destination	68.183.119.19
Destination Port	502
Signature	Connection to Honeypot
Source Port	38572
Sensor	70277776-34f4-11eb-9670-b2e6b8a57885

Transport	TCP
Severity	Medium

The exploit severity for this honeypot is medium. This suggests that no remote shells were open to the honeypot, unlike Kippo which emulates SSH. This does not mean no SSH will never be opened. No attackers opened an SSH yet on this instance. The severity of events will most likely stay medium until an SSH connection is opened.

4 Conclusion

The Kippo honeypots produced a more satisfying result as much more data was gathered. The Conpot honeypots emulated more services compared to Kippo, yet less data was collected. This suggests that more attackers target ordinary users or in general only attempt to use the SSH by gaining access through brute force attacks.

Conpot in comparison to Kippo emulates only industrial services to trick malicious users into thinking they had located an industrial complex. Industries are more difficult to gain access to and are more risky, as higher resource count means higher security and greater risk of exposure.

In total, including all Kippo and Conpot honeypots since deployment date, there have been 2,005,456 attacks registered on the Modern Honey Network. Out of this number, Splunk has shown top 10 URL in the home dashboard. The URLs were used to open an SSH connection by remotely executing an exploit through server directories. The URL list can be found in table 9 below.

Table 9 – Top URLs

URL	Sensor	Count
http://104.140.242.38/sh	cowrie	420
ftp://anonymous:anonymous@104.140.242.38/.sh	cowrie	210
http://119.147.213.57/bot.pl	cowrie	192
http://172.245.36.161/sh	cowrie	178
http://192.210.170.111/bins.sh	cowrie	168
http://193.109.217.15/bins/Astra.x86	cowrie	148
http://198.98.61.43/bdExploit/exploit.x86_64	cowrie	120
http://51.195.10.26/we.sh	cowrie	113
http://45.14.224.170/bin.sh	cowrie	100
http://192.210.170.111/bins/Astra.x86	cowrie	96

There were no high severity events registered on the Conpot honeypot. The Kippo honeypot has received multiple high severity event alerts due to an SSH connection being opened to the honeypot. However, Kippo is designed to emulate SSH services and capture brute force attacks. Brute force attacks are one of the simplest attacks to launch and therefore more users were attracted to the Kippo honeypots.

Conpot honeypots in comparison are quite different to Kippo. They may have a lower attacker base due to emulating industrial services. Malicious users who wish to target industries specifically, will be more interested in attacking the Conpot sensors. Industrial complexes require more time and skill to exploit which may discourage certain attackers. A risk of identity and location exposure is also greater if the attacker does not disguise correctly.

All the factors mentioned above may have been a partial reason why Kippo honeypots presented a much greater result than Conpot honeypots. Although it is not fully accurate, and it is partially biased to compare Kippo and Conpot as they are not the same types of honeypots.

Annex A – References

- *CONPOT – LOW INTERACTION SERVER-SIDE ICS HONEYPOT* (no date) available at: https://www.honeynet.org/projects/active/conpot/

- *CONPOT ICS/SCADA Honeypot* (no date) available at: http://conpot.org/

- SK, (2020) 'Kippo – A SSH Honeypot to Monitor Brute Force Attacks on Debian 7 / Ubuntu 13.10' available at: https://www.unixmen.com/kippo-ssh-honeypot-monitor-brute-force-attacks-debian-7-ubuntu-13-10/

- *KIPPO* (no date) available at: https://www.honeynet.org/projects/old/kippo/

- d1str0, (2020) 'pwnlandia/mhn' available at: https://github.com/pwnlandia/mhn

- Droplets which were used for hosting the honeypots and MHN are available here: https://www.digitalocean.com/

Annex B – Methodology

Term	Definition
Brute Force Attack	Automated repetitive login attempts using different credentials.
Conpot	Low interactive server-side Industrial Control Systems honeypot.
Emulate	Reproduce the function or action.
Honeypots	The VM which is generated and deployed on the Modern Honey Network.
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP Address	Internet Protocol address
Kippo	A medium interaction SSH honeypot designed to log brute force attacks.
MHN Dashboard	Control panel for the Modern Honey Network application.
Modern Honey Network (MHN)	Software which simplifies deployment of honeypots.
Port	An entry way to the system.
Splunk Console	Splunk control panel used to access collected data.
SSH	Secure Shell