Fifteen Months in the Life of a Honeyfarm

Cristian Munteanu, Said Jawad Saidi,
Oliver Gasser, Georgios Smaragdakis*, Anja Feldmann

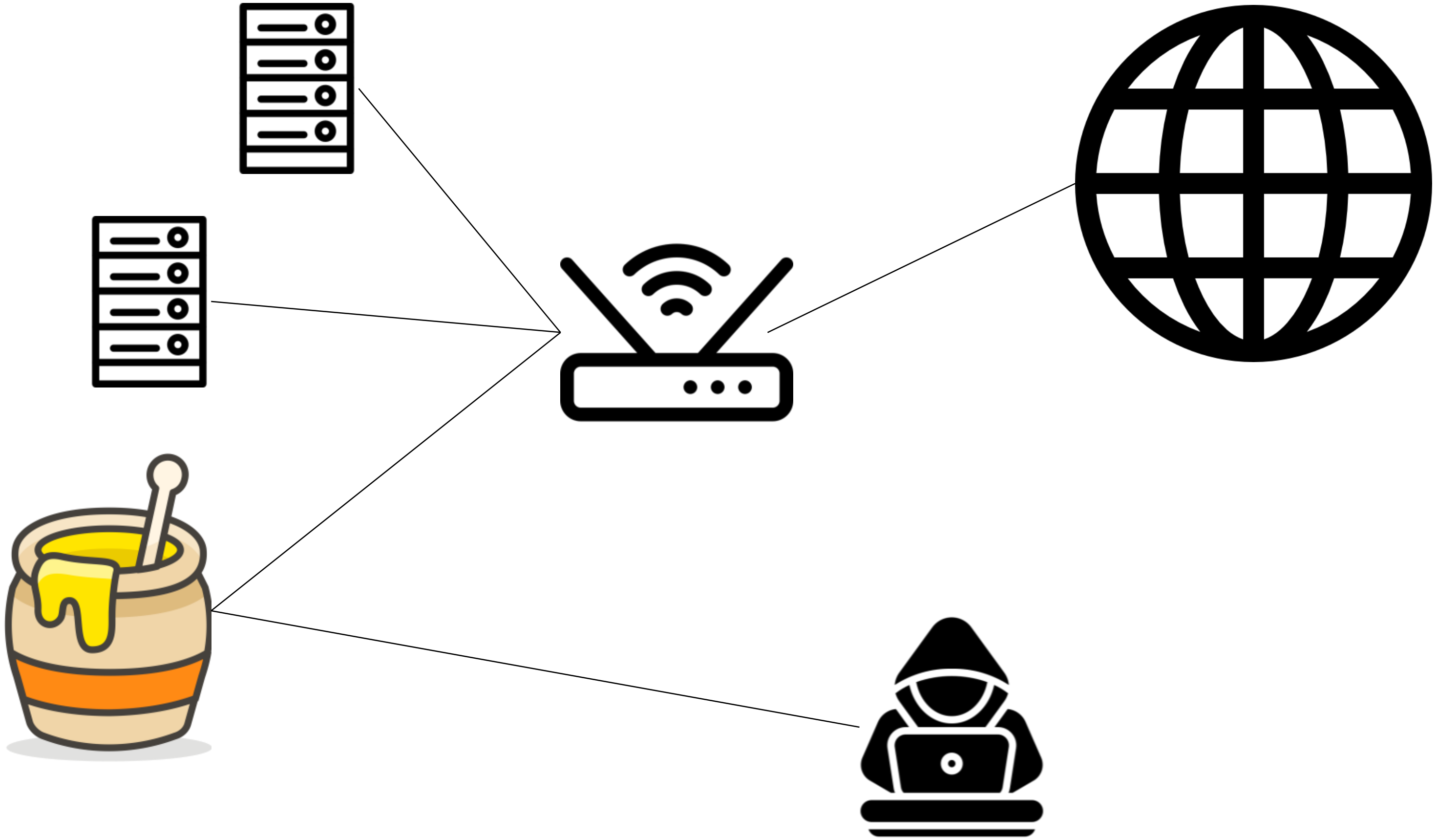
Max Planck Institute for Informatics, *TU Delft

max planck institut
informatik

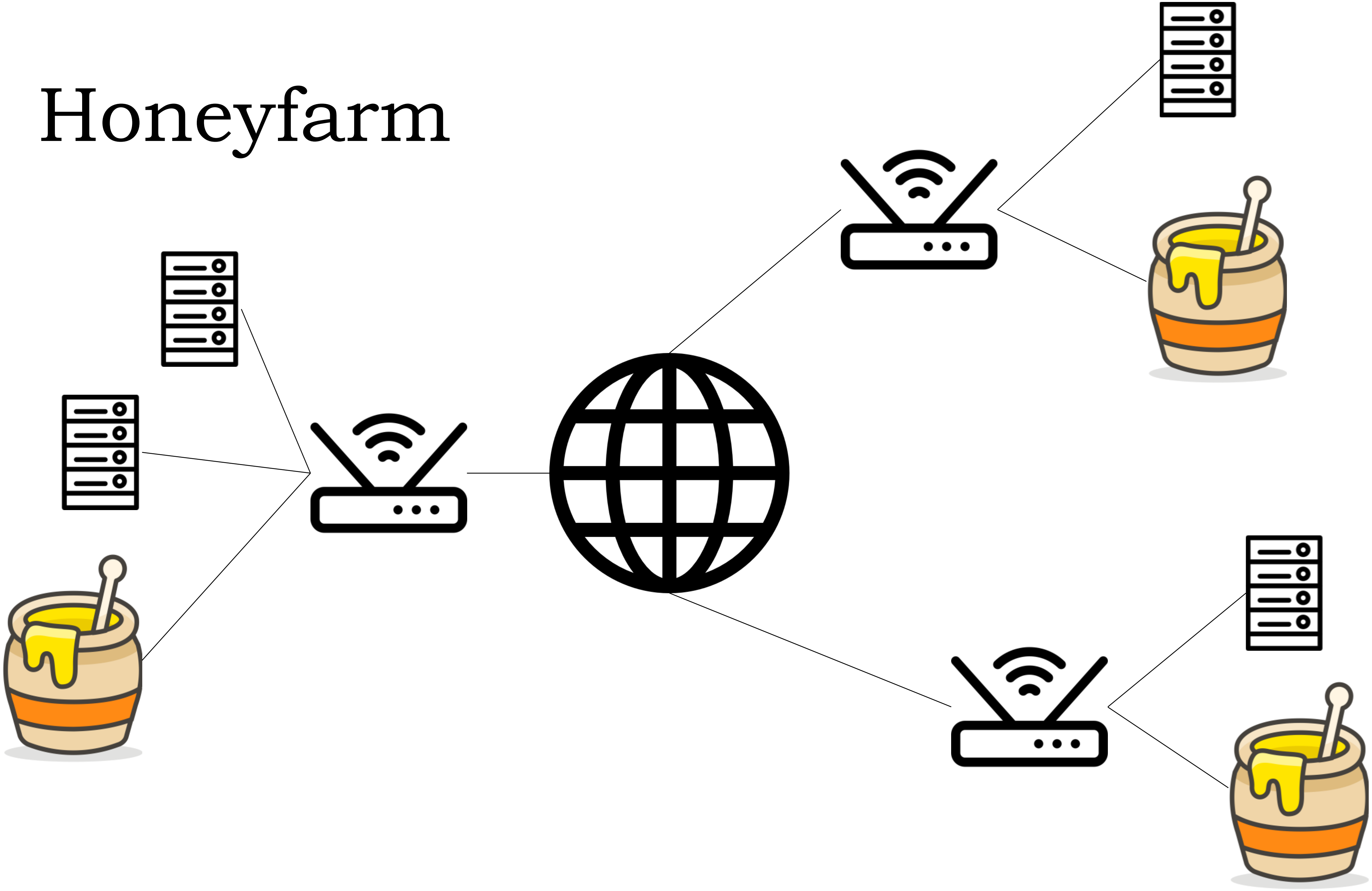
GLOBAL
CYBER
ALLIANCE™

TU Delft

Honeypot



Honeyfarm



Previous work

- *SCADA security using SSH honeypot* (2019)

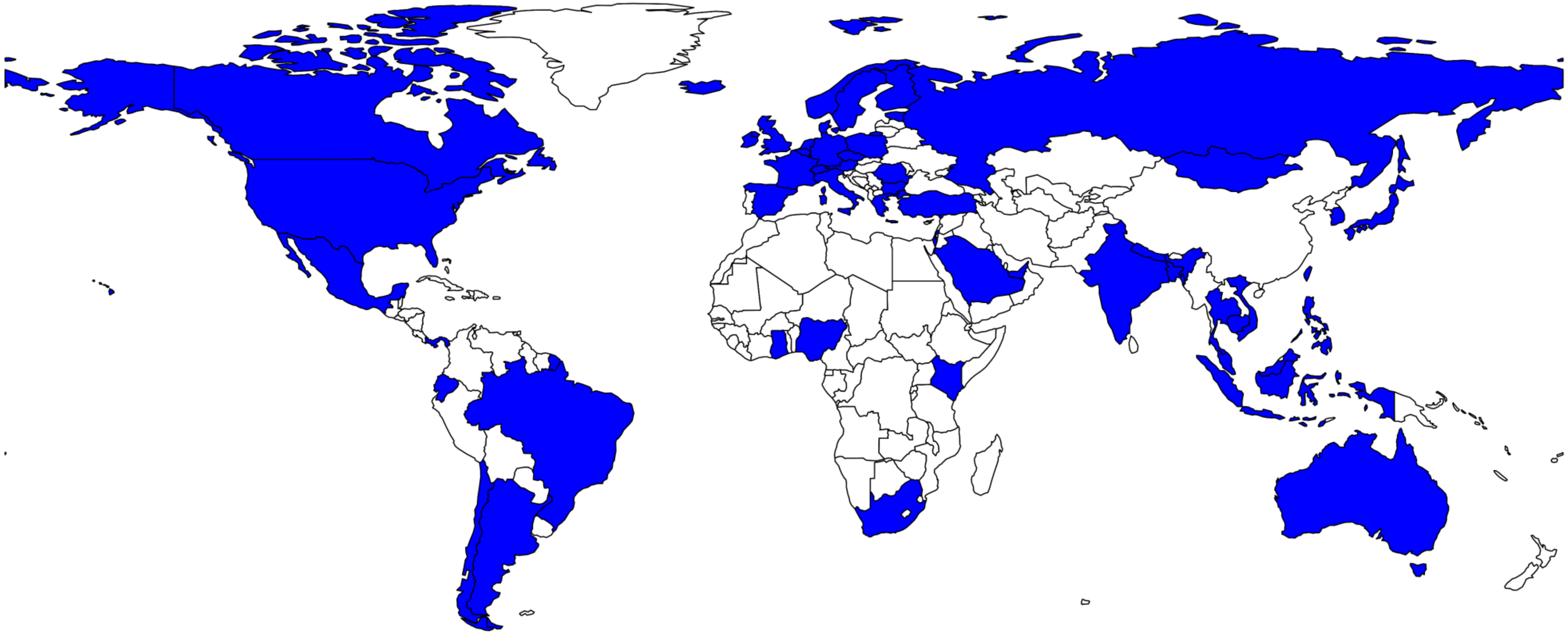
  Belqruch et al.
- *Study of Internet Threats and Attack Methods Using Honeypots and Honeynets* (2014)

  Sochor et al.
- *Patterns and Patter - An Investigation into SSH Activity Using Kippo Honeypots* (2013)

  Valli et al.

GLOBAL CYBER ALLIANCE™

GCA Honeyfarm



221 Honeypots - 55 Countries, 65 Networks

Collected Data

- Login Credentials
- Executed Commands
- Hashes of created/downloaded/generated Files

Top 10 `root` passwords

- admin
- 1234
- 3245gs5662d34
- dreambox
- vertex25ektks123
- 12345
- h3c
- 1qaz2wsx3edc
- passw0rd
- GM8182

Top 10 `root` passwords

- **admin**
- **1234**
- 3245gs5662d34
- **dreambox**
- vertex25ektks123
- **12345**
- h3c
- **1qaz2wsx3edc**
- **passw0rd**
- GM8182

Top 10 `root` passwords

- admin
- 1234
- **3245gs5662d34**
- dreambox
- **vertex25ektks123**
- 12345
- **h3c**
- 1qaz2wsx3edc
- passw0rd
- **GM8182**

Top 10 `root` passwords

- admin
- 1234
- **3245gs5662d34**
- dreambox
- **vertex25ektks123**
- 12345
- **h3c**
- 1qaz2wsx3edc
- passw0rd
- **GM8182**

There is a coordination between intruders!

Commands (top 30)

Commands		
grep name	awk	cat /proc/cpuinfo
free -m	crontab -l	w (whois)
uname -a	bash	chpasswd
mkdir .ssh	rm -rf .ssh	chmod -R go= /.ssh
top	echo "ssh-rsa AAA...“ » .ssh/authorized_keys	
shell	cat /proc/mounts	wget
tftp	history -c	chmod 777 bins.sh

Commands (top 30)

Commands		
grep name	awk	cat /proc/cpuinfo
free -m	crontab -l	w (whois)
uname -a	bash	chpasswd
mkdir .ssh	rm -rf .ssh	chmod -R go= /.ssh
top	echo "ssh-rsa AAA…“ » .ssh/authorized_keys	
shell	cat /proc/mounts	wget
tftp	history -c	chmod 777 bins.sh

Commands (top 30)

Commands		
grep name	awk	cat /proc/cpuinfo
free -m	crontab -l	w (whois)
uname -a	bash	chpasswd
mkdir .ssh	rm -rf .ssh	chmod -R go= /.ssh
top	echo "ssh-rsa AAA...“ » .ssh/authorized_keys	
shell	cat /proc/mounts	wget
tftp	history -c	chmod 777 bins.sh

Commands (top 30)

Commands		
grep name	awk	cat /proc/cpuinfo
free -m	crontab -l	w (whois)
uname -a	bash	chpasswd
mkdir .ssh	rm -rf .ssh	chmod -R go= /.ssh
top	echo "ssh-rsa AAA...“ » .ssh/authorized_keys	
shell	cat /proc/mounts	wget
tftp	history -c	chmod 777 bins.sh

Commands (top 30)

Commands		
grep name	awk	cat /proc/cpuinfo
free -m	crontab -l	w (whois)
uname -a	bash	chpasswd
mkdir .ssh	rm -rf .ssh	chmod -R go= /.ssh
top	echo "ssh-rsa AAA...“ » .ssh/authorized_keys	
shell	cat /proc/mounts	wget
tftp	history -c	chmod 777 bins.sh

Commands (top 30)

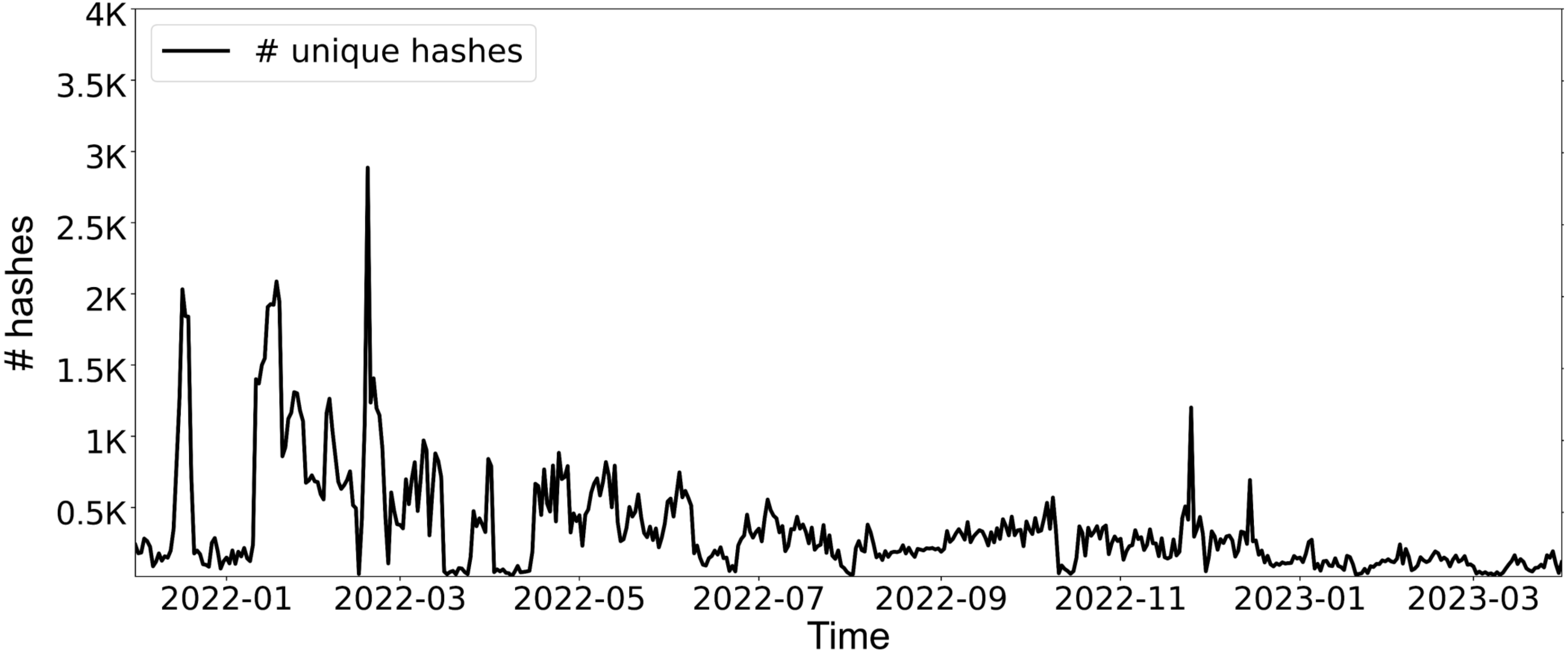
Commands		
grep name	awk	cat /proc/cpuinfo
free -m	crontab -l	w (whois)
uname -a	bash	chpasswd
mkdir .ssh	rm -rf .ssh	chmod -R go= /.ssh
top	echo "ssh-rsa AAA...“ » .ssh/authorized_keys	
shell	cat /proc/mounts	wget
tftp	history -c	chmod 777 bins.sh

Commands (top 30)

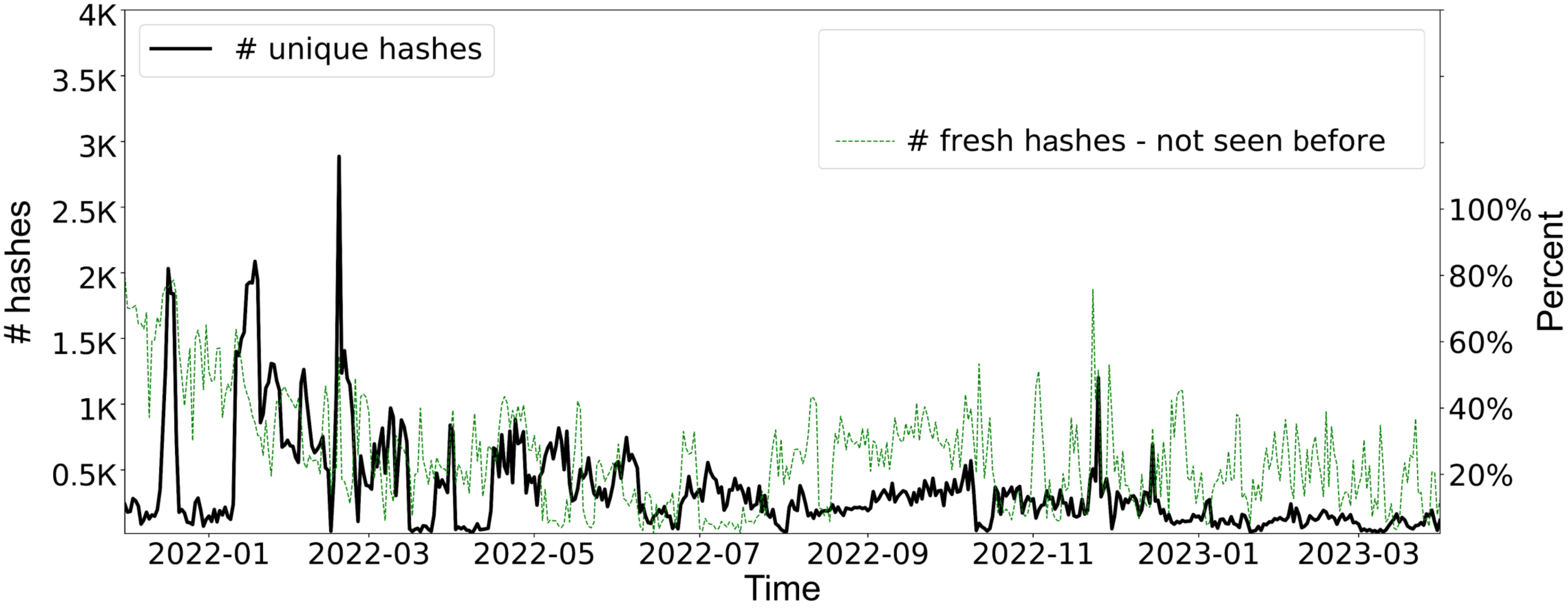
Commands		
grep name	awk	cat /proc/cpuinfo
free -m	crontab -l	w (whois)
uname -a	bash	chpasswd
mkdir .ssh	rm -rf .ssh	chmod -R go= /.ssh
top	echo "ssh-rsa AAA...“ » .ssh/authorized_keys	
shell	cat /proc/mounts	wget
tftp	history -c	chmod 777 bins.sh

Attacks are complex!

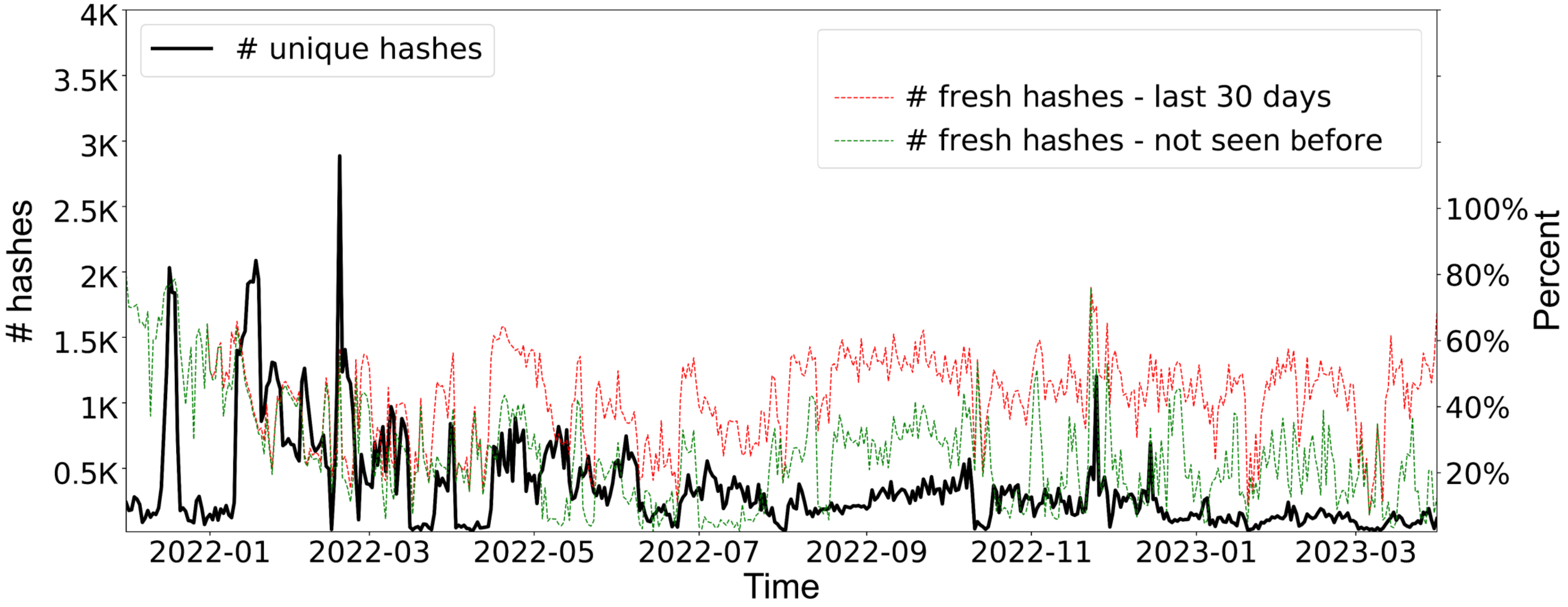
Files and Hashes



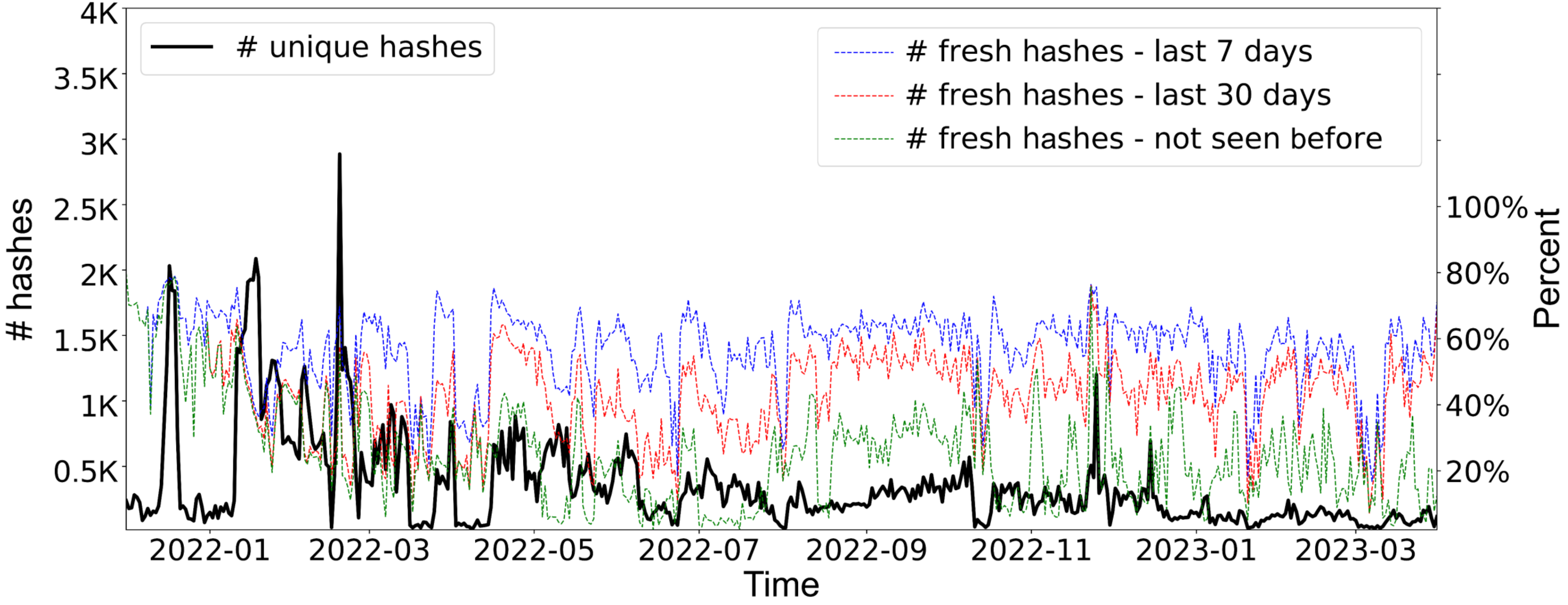
Files and Hashes



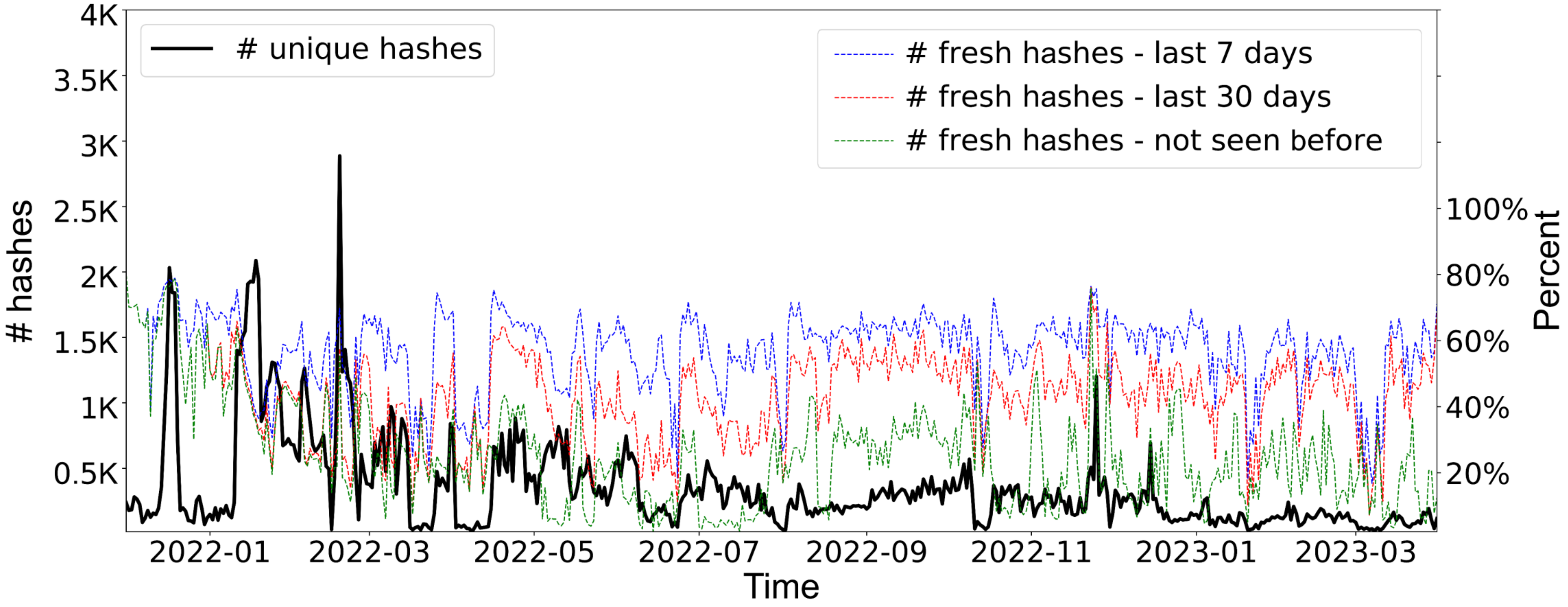
Files and Hashes



Files and Hashes

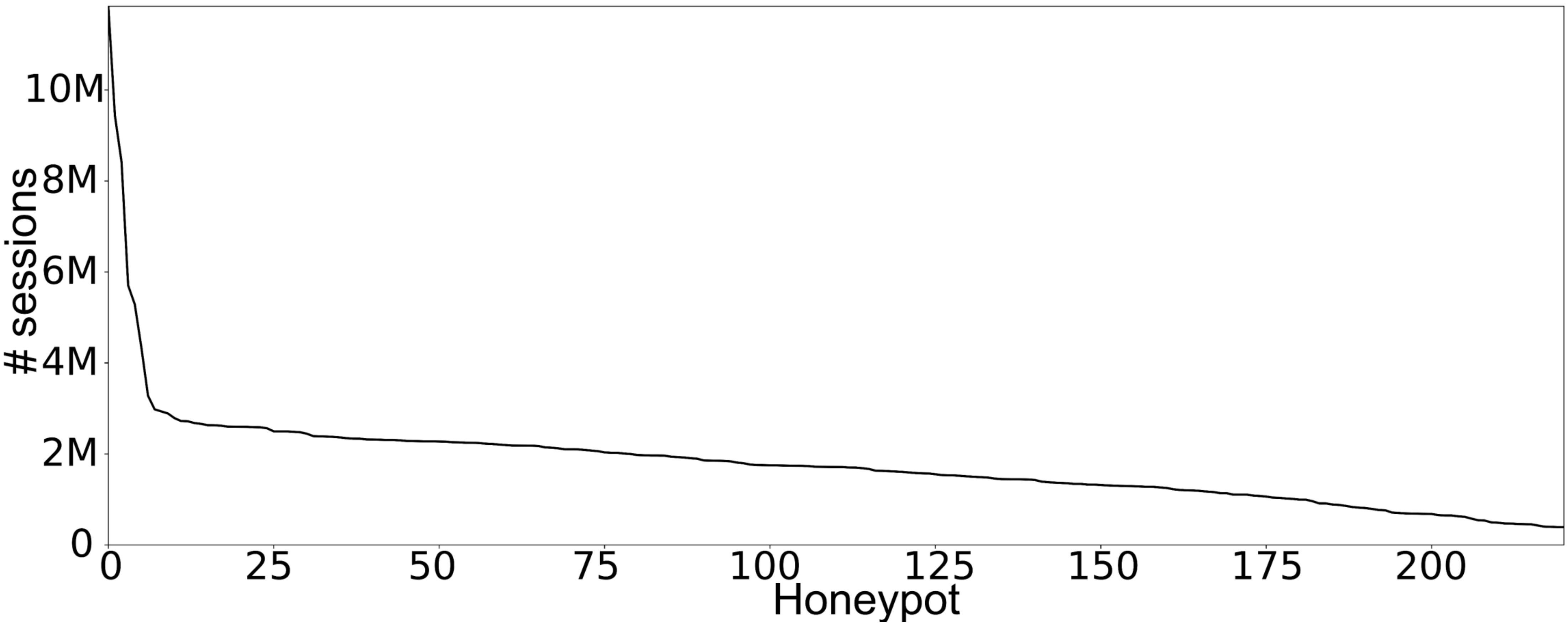


Files and Hashes

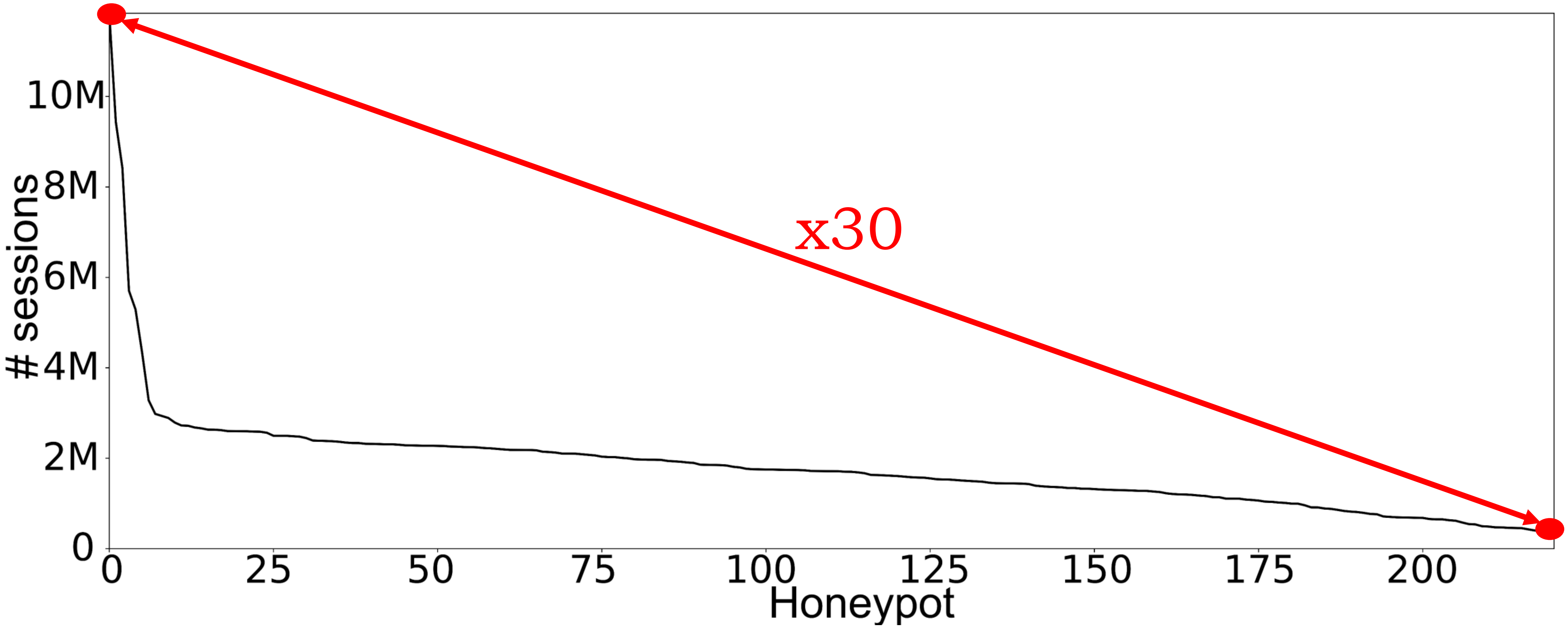


Attacks are coming in waves!

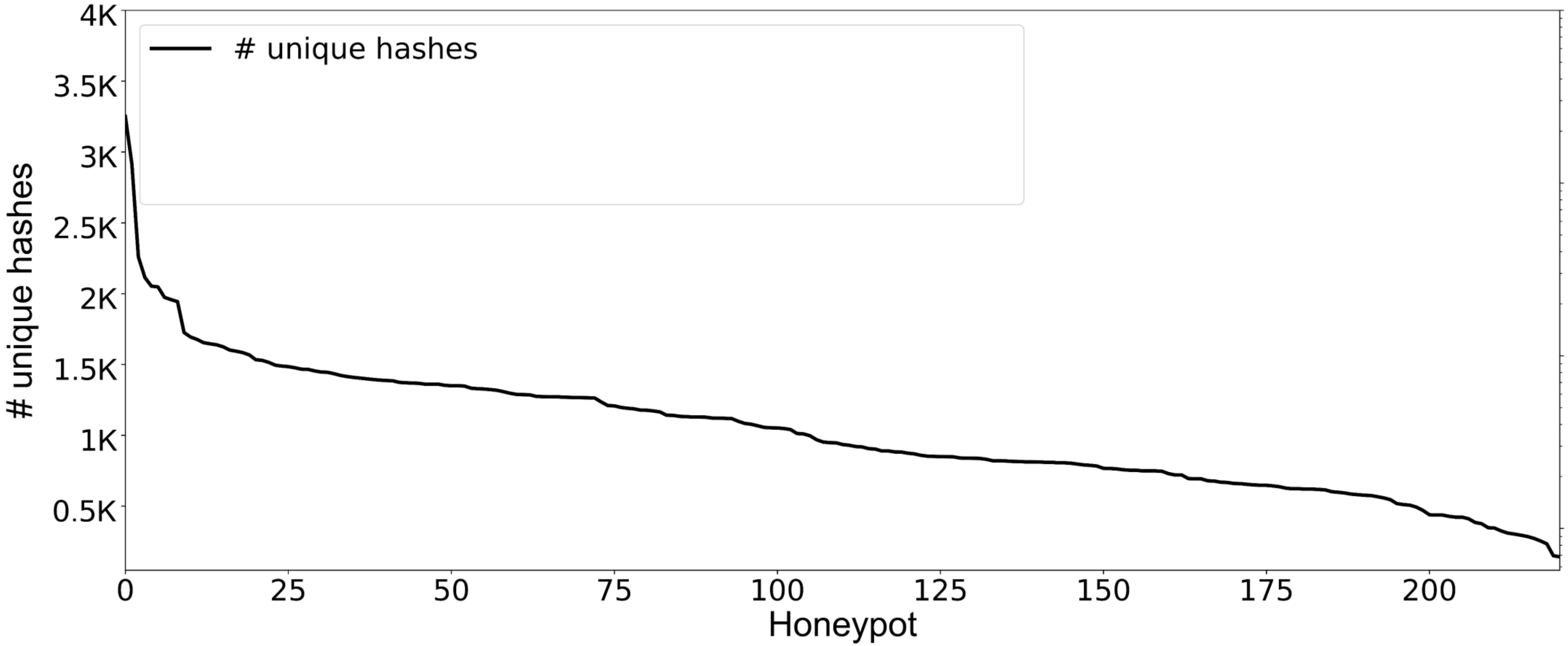
Sessions per Honeypot



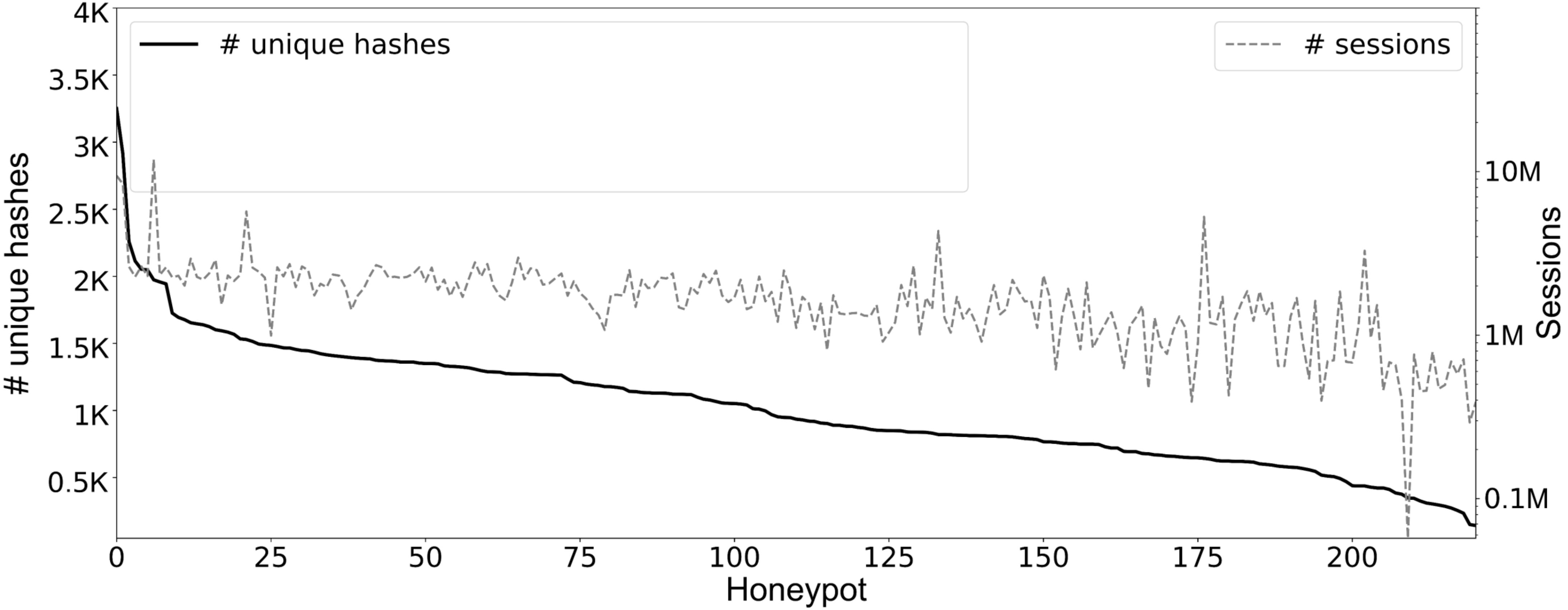
Sessions per Honeypot



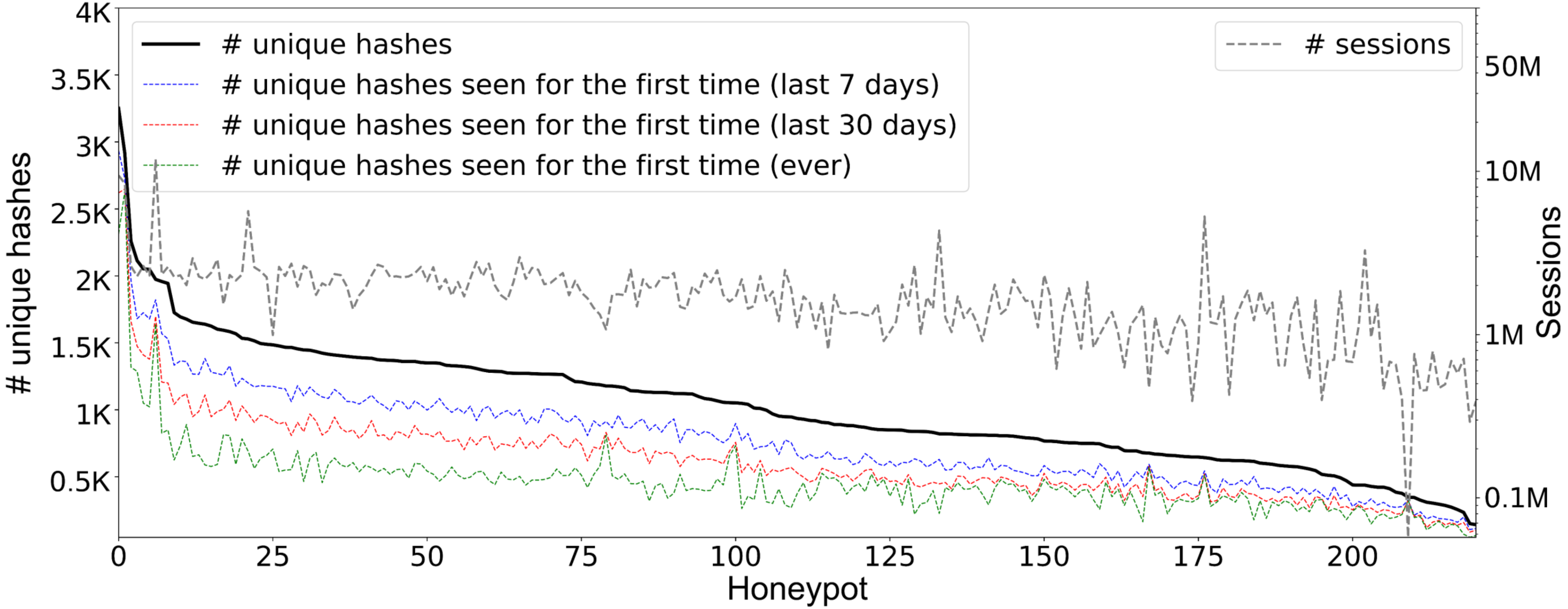
Unique Hashes per Honeypot



Unique Hashes per Honeypot



Unique Hashes per Honeypot



Number and distribution matter!

Files and Hashes

Hash	# Sessions	# Unique IP	# Days	Tag	# Honeypots
H1	25,688,228	118,924	484	trojan	221
H2	153,672	3	252	malicious	202
H3	110,280	12,698	119	trojan	150
H4	105,102	1,288	20	mirai	203
H5	96,523	1,027	451	mirai	221

Files and Hashes

Hash	# Sessions	# Unique IP	# Days	Tag	# Honeypots
H1	25,688,228	118,924	484	trojan	221
H2	153,672	3	252	malicious	202
H3	110,280	12,698	119	trojan	150
H4	105,102	1,288	20	mirai	203
H5	96,523	1,027	451	mirai	221

Files and Hashes

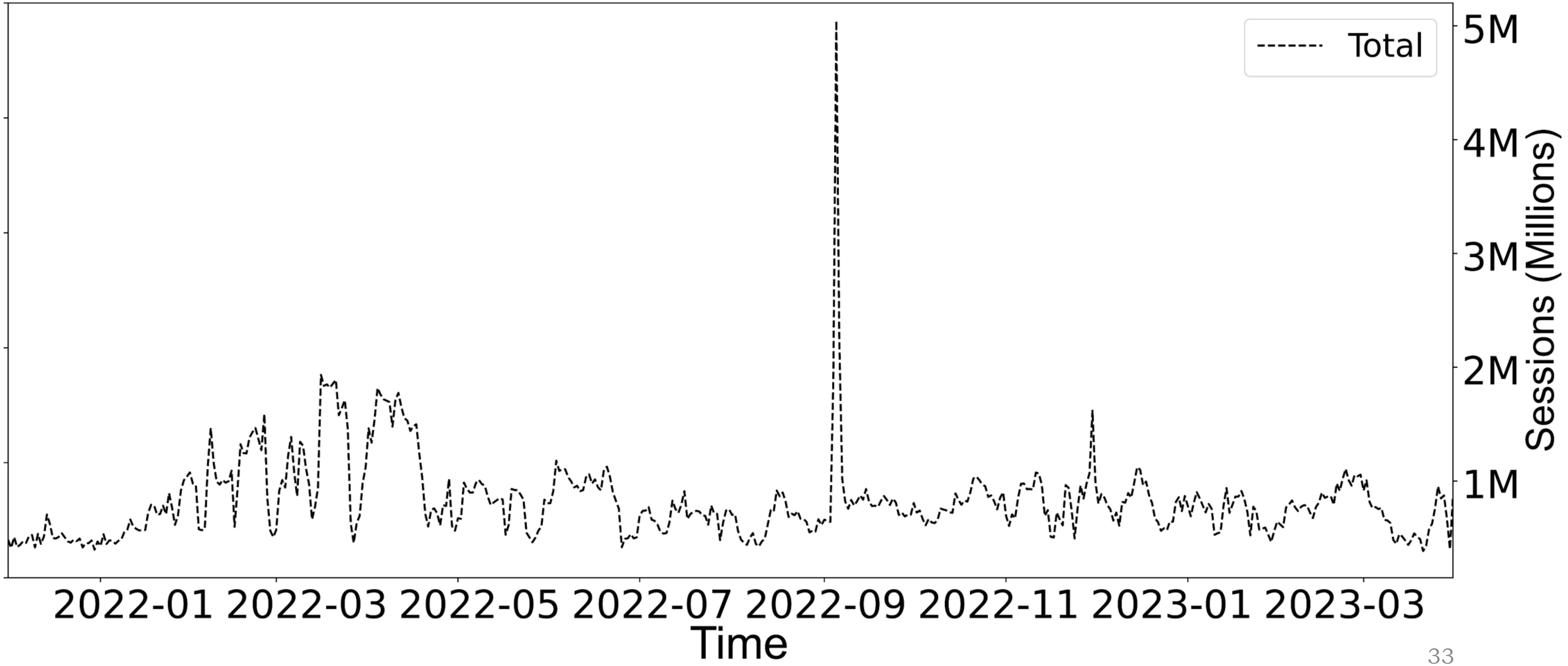
Hash	# Sessions	# Unique IP	# Days	Tag	# Honeypots
H1	25,688,228	118,924	484	trojan	221
H2	153,672	3	252	malicious	202
H3	110,280	12,698	119	trojan	150
H4	105,102	1,288	20	mirai	203
H5	96,523	1,027	451	mirai	221

Networks are unaware!

Summary

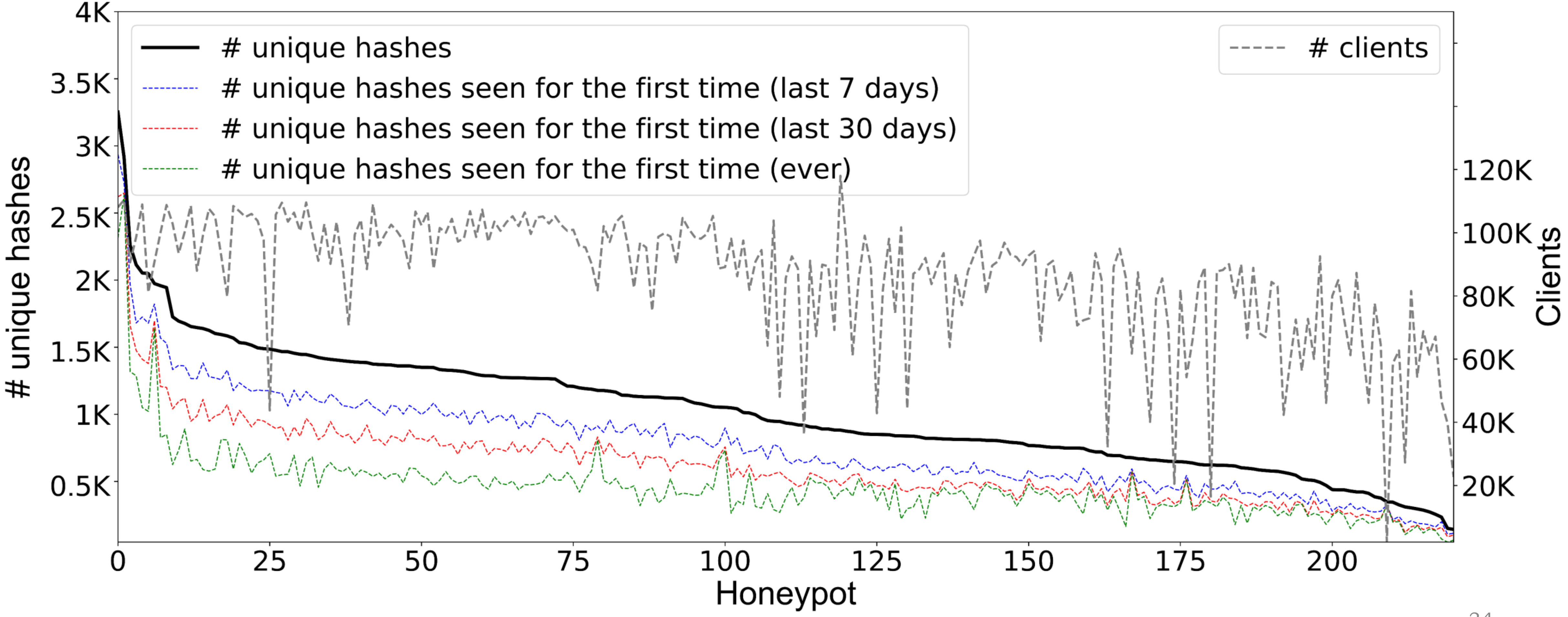
- Attacks are complex and coordinated
- Every Honeypot counts
- Honeyfarms and security reality

Sessions



Total
5M
4M
3M
2M
1M
Sessions (Millions)
2022-01
2022-03
2022-05
2022-07
2022-09
2022-11
2023-01
2023-03
Time

Unique Hashes per Honeypot


# unique hashes
# unique hashes seen for the first time (last 7 days)
# unique hashes seen for the first time (last 30 days)
# unique hashes seen for the first time (ever)
# clients
4K
3.5K
3K
2.5K
2K
1.5K
1K
0.5K
# unique hashes
120K
100K
80K
60K
40K
20K
Clients
Honeypot