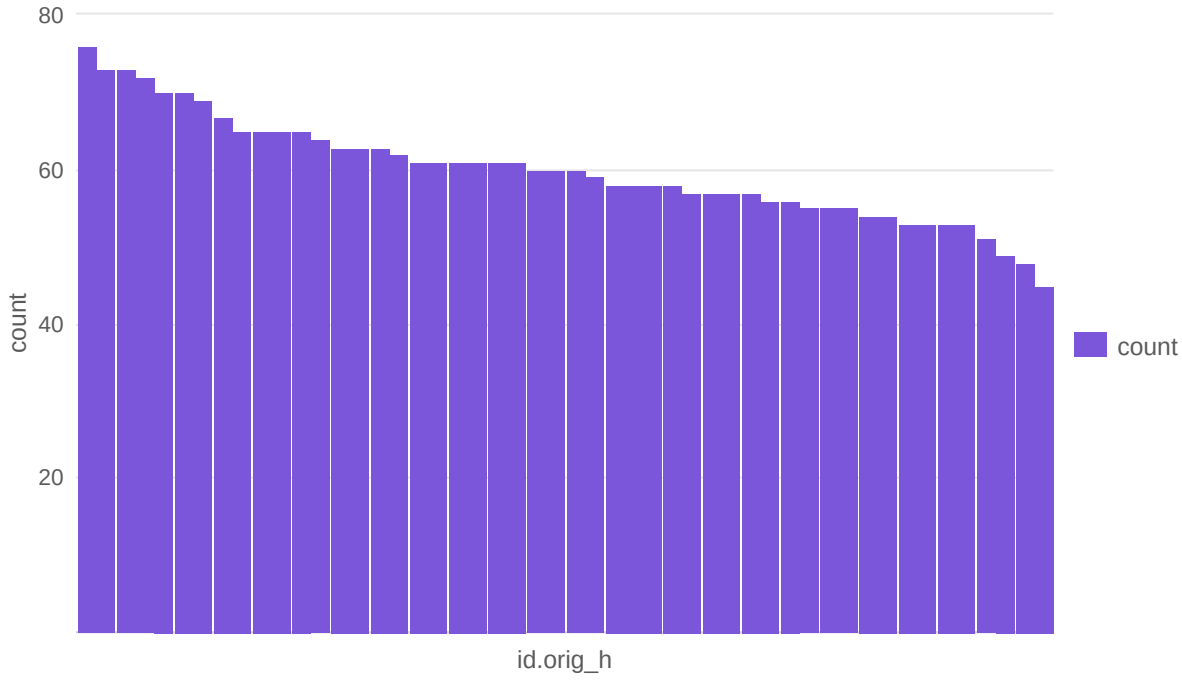
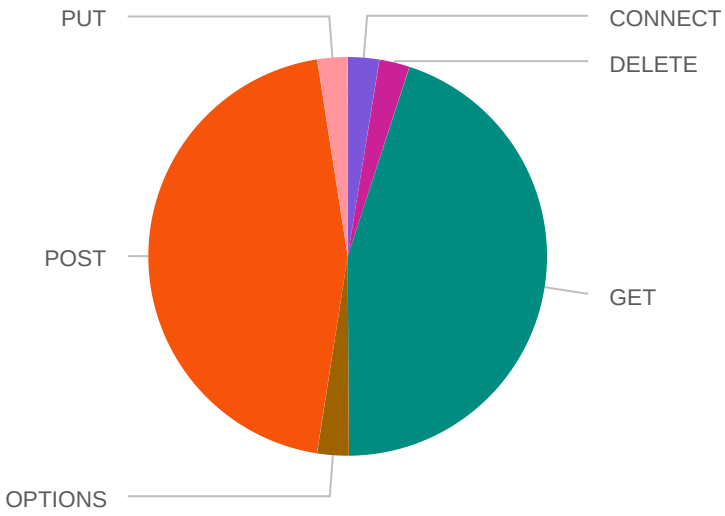
Top Active Source Ips



HTTP Methods Used



Suspicious User Agents

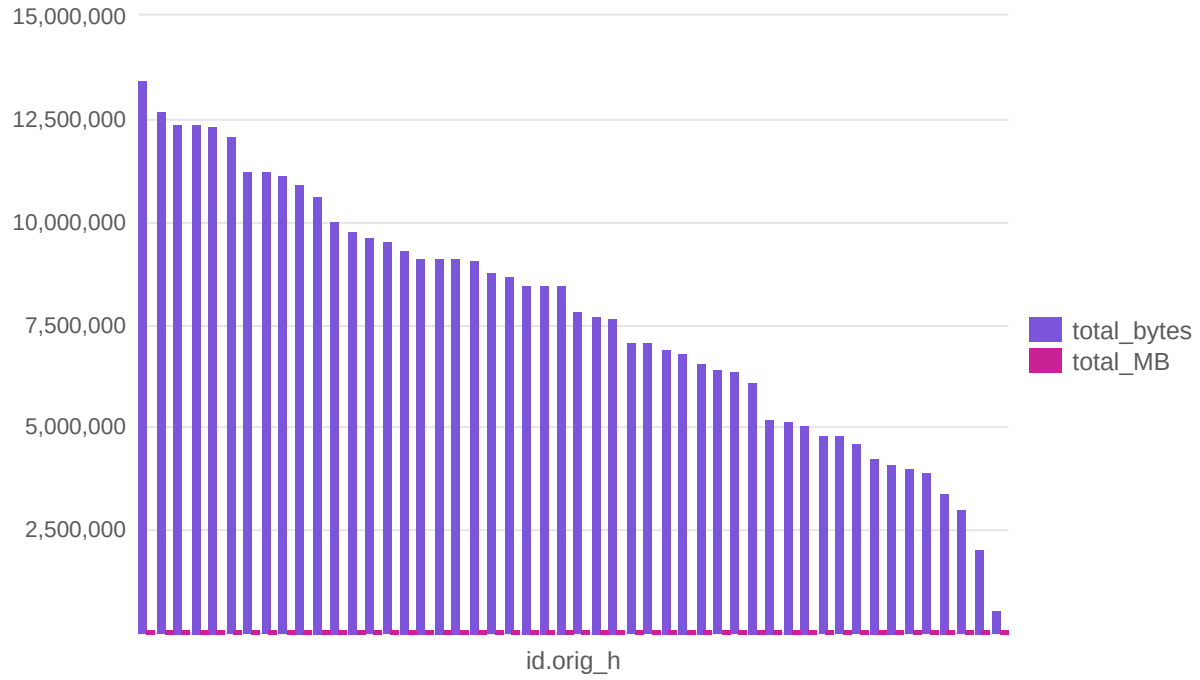
user_agent	id.orig_h	count
botnet-checker/1.0	10.0.0.15	5
python-requests/2.25.1	10.0.0.18	5
curl/7.68.0	10.0.0.13	4
curl/7.68.0	10.0.0.40	4
python-requests/2.25.1	10.0.0.34	4
python-requests/2.25.1	10.0.0.41	4
sqlmap/1.5.1	10.0.0.19	4
sqlmap/1.5.1	10.0.0.31	4
sqlmap/1.5.1	10.0.0.47	4
sqlmap/1.5.1	10.0.0.57	4
botnet-checker/1.0	10.0.0.14	3
botnet-checker/1.0	10.0.0.25	3
botnet-checker/1.0	10.0.0.28	3
botnet-checker/1.0	10.0.0.31	3
botnet-checker/1.0	10.0.0.49	3
botnet-checker/1.0	10.0.0.54	3
botnet-checker/1.0	10.0.0.56	3
curl/7.68.0	10.0.0.16	3
curl/7.68.0	10.0.0.17	3
curl/7.68.0	10.0.0.31	3
curl/7.68.0	10.0.0.47	3
python-requests/2.25.1	10.0.0.22	3
python-requests/2.25.1	10.0.0.25	3
python-requests/2.25.1	10.0.0.27	3
python-requests/2.25.1	10.0.0.32	3
python-requests/2.25.1	10.0.0.37	3
python-requests/2.25.1	10.0.0.39	3
python-requests/2.25.1	10.0.0.45	3
python-requests/2.25.1	10.0.0.46	3
python-requests/2.25.1	10.0.0.50	3
python-requests/2.25.1	10.0.0.52	3
sqlmap/1.5.1	10.0.0.10	3
sqlmap/1.5.1	10.0.0.11	3
sqlmap/1.5.1	10.0.0.17	3
sqlmap/1.5.1	10.0.0.21	3
sqlmap/1.5.1	10.0.0.22	3
sqlmap/1.5.1	10.0.0.28	3
sqlmap/1.5.1	10.0.0.42	3
sqlmap/1.5.1	10.0.0.46	3
sqlmap/1.5.1	10.0.0.53	3
botnet-checker/1.0	10.0.0.11	2
botnet-checker/1.0	10.0.0.20	2
botnet-checker/1.0	10.0.0.29	2
botnet-checker/1.0	10.0.0.32	2
botnet-checker/1.0	10.0.0.35	2
botnet-checker/1.0	10.0.0.36	2
botnet-checker/1.0	10.0.0.38	2
botnet-checker/1.0	10.0.0.39	2
botnet-checker/1.0	10.0.0.41	2
botnet-checker/1.0	10.0.0.42	2

user_agent	id.orig_h	count
botnet-checker/1.0	10.0.0.43	2
botnet-checker/1.0	10.0.0.46	2
botnet-checker/1.0	10.0.0.59	2
curl/7.68.0	10.0.0.10	2
curl/7.68.0	10.0.0.15	2
curl/7.68.0	10.0.0.20	2
curl/7.68.0	10.0.0.22	2
curl/7.68.0	10.0.0.23	2
curl/7.68.0	10.0.0.27	2
curl/7.68.0	10.0.0.35	2
curl/7.68.0	10.0.0.38	2
curl/7.68.0	10.0.0.39	2
curl/7.68.0	10.0.0.42	2
curl/7.68.0	10.0.0.51	2
curl/7.68.0	10.0.0.56	2
curl/7.68.0	10.0.0.57	2
python-requests/2.25.1	10.0.0.13	2
python-requests/2.25.1	10.0.0.16	2
python-requests/2.25.1	10.0.0.19	2
python-requests/2.25.1	10.0.0.24	2
python-requests/2.25.1	10.0.0.29	2
python-requests/2.25.1	10.0.0.36	2
python-requests/2.25.1	10.0.0.38	2
python-requests/2.25.1	10.0.0.40	2
python-requests/2.25.1	10.0.0.47	2
python-requests/2.25.1	10.0.0.48	2
sqlmap/1.5.1	10.0.0.16	2
sqlmap/1.5.1	10.0.0.29	2
sqlmap/1.5.1	10.0.0.35	2
sqlmap/1.5.1	10.0.0.36	2
sqlmap/1.5.1	10.0.0.45	2
sqlmap/1.5.1	10.0.0.50	2
sqlmap/1.5.1	10.0.0.52	2
sqlmap/1.5.1	10.0.0.56	2
sqlmap/1.5.1	10.0.0.59	2
botnet-checker/1.0	10.0.0.10	1
botnet-checker/1.0	10.0.0.12	1
botnet-checker/1.0	10.0.0.13	1
botnet-checker/1.0	10.0.0.18	1
botnet-checker/1.0	10.0.0.23	1
botnet-checker/1.0	10.0.0.24	1
botnet-checker/1.0	10.0.0.26	1
botnet-checker/1.0	10.0.0.30	1
botnet-checker/1.0	10.0.0.40	1
botnet-checker/1.0	10.0.0.44	1
botnet-checker/1.0	10.0.0.45	1
botnet-checker/1.0	10.0.0.48	1
botnet-checker/1.0	10.0.0.50	1
botnet-checker/1.0	10.0.0.51	1
botnet-checker/1.0	10.0.0.52	1
botnet-checker/1.0	10.0.0.55	1
botnet-checker/1.0	10.0.0.57	1

user_agent	id.orig_h	count
botnet-checker/1.0	10.0.0.58	1
curl/7.68.0	10.0.0.11	1
curl/7.68.0	10.0.0.12	1
curl/7.68.0	10.0.0.14	1
curl/7.68.0	10.0.0.18	1
curl/7.68.0	10.0.0.21	1
curl/7.68.0	10.0.0.24	1
curl/7.68.0	10.0.0.26	1
curl/7.68.0	10.0.0.28	1
curl/7.68.0	10.0.0.29	1
curl/7.68.0	10.0.0.30	1
curl/7.68.0	10.0.0.33	1
curl/7.68.0	10.0.0.34	1
curl/7.68.0	10.0.0.36	1
curl/7.68.0	10.0.0.43	1
curl/7.68.0	10.0.0.44	1
curl/7.68.0	10.0.0.45	1
curl/7.68.0	10.0.0.46	1
curl/7.68.0	10.0.0.48	1
curl/7.68.0	10.0.0.49	1
curl/7.68.0	10.0.0.50	1
curl/7.68.0	10.0.0.55	1
curl/7.68.0	10.0.0.58	1
curl/7.68.0	10.0.0.59	1
python-requests/2.25.1	10.0.0.10	1
python-requests/2.25.1	10.0.0.12	1
python-requests/2.25.1	10.0.0.14	1
python-requests/2.25.1	10.0.0.17	1
python-requests/2.25.1	10.0.0.21	1
python-requests/2.25.1	10.0.0.23	1
python-requests/2.25.1	10.0.0.33	1
python-requests/2.25.1	10.0.0.42	1
python-requests/2.25.1	10.0.0.43	1
python-requests/2.25.1	10.0.0.53	1
python-requests/2.25.1	10.0.0.55	1
python-requests/2.25.1	10.0.0.56	1
python-requests/2.25.1	10.0.0.57	1
python-requests/2.25.1	10.0.0.58	1
python-requests/2.25.1	10.0.0.59	1
sqlmap/1.5.1	10.0.0.14	1
sqlmap/1.5.1	10.0.0.15	1
sqlmap/1.5.1	10.0.0.18	1
sqlmap/1.5.1	10.0.0.24	1
sqlmap/1.5.1	10.0.0.25	1
sqlmap/1.5.1	10.0.0.26	1
sqlmap/1.5.1	10.0.0.27	1
sqlmap/1.5.1	10.0.0.30	1
sqlmap/1.5.1	10.0.0.32	1
sqlmap/1.5.1	10.0.0.37	1
sqlmap/1.5.1	10.0.0.39	1
sqlmap/1.5.1	10.0.0.40	1
sqlmap/1.5.1	10.0.0.41	1

user_agent	id.orig_h	count
sqlmap/1.5.1	10.0.0.43	1
sqlmap/1.5.1	10.0.0.44	1
sqlmap/1.5.1	10.0.0.48	1
sqlmap/1.5.1	10.0.0.54	1
sqlmap/1.5.1	10.0.0.55	1

Large Data Transfers



Potentially Compromised Hosts

id.orig_h	activities
10.0.0.10	Client Error Large Transfer Server Error Standard Suspicious Agent Unexpected Method
10.0.0.11	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.12	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.13	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.14	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.15	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.16	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.17	Client Error Large Transfer Server Error Standard Suspicious Agent Unexpected Method
10.0.0.18	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.19	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method

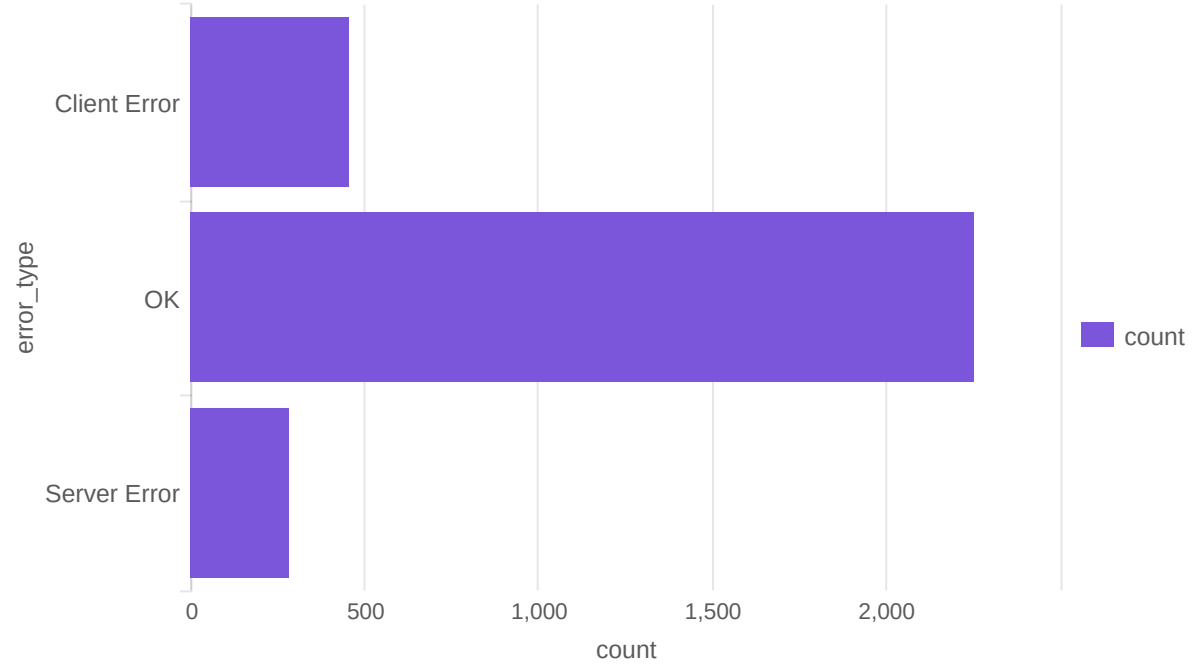
id.orig_h	activities
10.0.0.20	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.21	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.22	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.23	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.24	Client Error Large Transfer Server Error Standard Suspicious Agent Unexpected Method
10.0.0.25	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.26	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.27	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.28	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.29	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method

id.orig_h	activities
10.0.0.30	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.31	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.32	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.33	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.34	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.35	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.36	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.37	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.38	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.39	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method

id.orig_h	activities
10.0.0.40	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.41	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.42	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.43	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.44	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.45	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.46	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.47	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.48	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.49	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method

id.orig_h	activities
10.0.0.50	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.51	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.52	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.53	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.54	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.55	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.56	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.57	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.58	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method
10.0.0.59	Client Error Large Transfer Server Error Standard Suspicious Agent Suspicious Uri Unexpected Method

Error Trend



Suspicious URIs

uri	id.orig_h	count
/admin	10.0.0.12	1
/admin	10.0.0.14	1
/admin	10.0.0.19	1
/admin	10.0.0.20	2
/admin	10.0.0.22	1
/admin	10.0.0.25	2
/admin	10.0.0.27	1
/admin	10.0.0.28	2
/admin	10.0.0.31	1
/admin	10.0.0.34	1
/admin	10.0.0.35	2
/admin	10.0.0.36	1
/admin	10.0.0.38	2
/admin	10.0.0.39	1
/admin	10.0.0.40	1
/admin	10.0.0.42	1
/admin	10.0.0.44	1
/admin	10.0.0.46	3
/admin	10.0.0.48	1
/admin	10.0.0.49	1
/admin	10.0.0.52	3
/admin	10.0.0.53	1
/admin	10.0.0.54	3

uri	id.orig_h	count
/admin	10.0.0.55	1
/admin	10.0.0.57	2
/admin	10.0.0.59	1
/config.php	10.0.0.12	1
/config.php	10.0.0.16	1
/config.php	10.0.0.20	1
/config.php	10.0.0.22	2
/config.php	10.0.0.25	1
/config.php	10.0.0.26	1
/config.php	10.0.0.28	1
/config.php	10.0.0.30	1
/config.php	10.0.0.32	1
/config.php	10.0.0.33	1
/config.php	10.0.0.34	1
/config.php	10.0.0.36	1
/config.php	10.0.0.37	1
/config.php	10.0.0.39	2
/config.php	10.0.0.42	3
/config.php	10.0.0.47	2
/config.php	10.0.0.48	1
/config.php	10.0.0.52	2
/config.php	10.0.0.55	1
/etc/passwd	10.0.0.12	2
/etc/passwd	10.0.0.14	1
/etc/passwd	10.0.0.15	1
/etc/passwd	10.0.0.18	1
/etc/passwd	10.0.0.19	1
/etc/passwd	10.0.0.21	1
/etc/passwd	10.0.0.25	1
/etc/passwd	10.0.0.26	1
/etc/passwd	10.0.0.27	2
/etc/passwd	10.0.0.28	1
/etc/passwd	10.0.0.29	1
/etc/passwd	10.0.0.30	3
/etc/passwd	10.0.0.31	1
/etc/passwd	10.0.0.32	1
/etc/passwd	10.0.0.33	1
/etc/passwd	10.0.0.37	2
/etc/passwd	10.0.0.39	1
/etc/passwd	10.0.0.40	1
/etc/passwd	10.0.0.41	1
/etc/passwd	10.0.0.43	1
/etc/passwd	10.0.0.44	1
/etc/passwd	10.0.0.45	1
/etc/passwd	10.0.0.46	2
/etc/passwd	10.0.0.48	2
/etc/passwd	10.0.0.52	1
/etc/passwd	10.0.0.53	1
/etc/passwd	10.0.0.54	1
/etc/passwd	10.0.0.58	1
/index.html	10.0.0.10	53
/index.html	10.0.0.11	45

uri	id.orig_h	count
/index.html	10.0.0.12	54
/index.html	10.0.0.13	62
/index.html	10.0.0.14	63
/index.html	10.0.0.15	58
/index.html	10.0.0.16	57
/index.html	10.0.0.17	61
/index.html	10.0.0.18	60
/index.html	10.0.0.19	53
/index.html	10.0.0.20	52
/index.html	10.0.0.21	59
/index.html	10.0.0.22	56
/index.html	10.0.0.23	53
/index.html	10.0.0.24	58
/index.html	10.0.0.25	61
/index.html	10.0.0.26	49
/index.html	10.0.0.27	68
/index.html	10.0.0.28	71
/index.html	10.0.0.29	53
/index.html	10.0.0.30	57
/index.html	10.0.0.31	69
/index.html	10.0.0.32	54
/index.html	10.0.0.33	53
/index.html	10.0.0.34	56
/index.html	10.0.0.35	58
/index.html	10.0.0.36	59
/index.html	10.0.0.37	55
/index.html	10.0.0.38	53
/index.html	10.0.0.39	59
/index.html	10.0.0.40	65
/index.html	10.0.0.41	43
/index.html	10.0.0.42	68
/index.html	10.0.0.43	46
/index.html	10.0.0.44	53
/index.html	10.0.0.45	67
/index.html	10.0.0.46	58
/index.html	10.0.0.47	61
/index.html	10.0.0.48	48
/index.html	10.0.0.49	60
/index.html	10.0.0.50	64
/index.html	10.0.0.51	56
/index.html	10.0.0.52	48
/index.html	10.0.0.53	55
/index.html	10.0.0.54	55
/index.html	10.0.0.55	57
/index.html	10.0.0.56	53
/index.html	10.0.0.57	55
/index.html	10.0.0.58	50
/index.html	10.0.0.59	49
/phpmyadmin	10.0.0.11	1
/phpmyadmin	10.0.0.13	1
/phpmyadmin	10.0.0.16	1
/phpmyadmin	10.0.0.19	1

uri	id.orig_h	count
/phpmyadmin	10.0.0.22	1
/phpmyadmin	10.0.0.26	1
/phpmyadmin	10.0.0.28	1
/phpmyadmin	10.0.0.31	2
/phpmyadmin	10.0.0.35	1
/phpmyadmin	10.0.0.39	1
/phpmyadmin	10.0.0.40	1
/phpmyadmin	10.0.0.43	1
/phpmyadmin	10.0.0.44	1
/phpmyadmin	10.0.0.45	1
/phpmyadmin	10.0.0.47	2
/phpmyadmin	10.0.0.48	1
/phpmyadmin	10.0.0.49	1
/phpmyadmin	10.0.0.51	1
/phpmyadmin	10.0.0.52	1
/phpmyadmin	10.0.0.57	1
/shell.php	10.0.0.11	2
/shell.php	10.0.0.12	2
/shell.php	10.0.0.14	1
/shell.php	10.0.0.15	2
/shell.php	10.0.0.20	1
/shell.php	10.0.0.30	1
/shell.php	10.0.0.32	1
/shell.php	10.0.0.35	1
/shell.php	10.0.0.36	2
/shell.php	10.0.0.39	1
/shell.php	10.0.0.40	1
/shell.php	10.0.0.41	1
/shell.php	10.0.0.44	1
/shell.php	10.0.0.46	1
/shell.php	10.0.0.50	1
/shell.php	10.0.0.51	1
/shell.php	10.0.0.54	1
/shell.php	10.0.0.55	1
/shell.php	10.0.0.56	1
/shell.php	10.0.0.58	2
/wp-admin	10.0.0.12	1
/wp-admin	10.0.0.13	2
/wp-admin	10.0.0.14	3
/wp-admin	10.0.0.16	1
/wp-admin	10.0.0.21	1
/wp-admin	10.0.0.23	1
/wp-admin	10.0.0.26	1
/wp-admin	10.0.0.27	1
/wp-admin	10.0.0.29	1
/wp-admin	10.0.0.30	1
/wp-admin	10.0.0.34	1
/wp-admin	10.0.0.38	2
/wp-admin	10.0.0.40	1
/wp-admin	10.0.0.42	1
/wp-admin	10.0.0.43	1
/wp-admin	10.0.0.45	1

uri	id.orig_h	count
/wp-admin	10.0.0.49	1
/wp-admin	10.0.0.50	2
/wp-admin	10.0.0.54	1
/wp-admin	10.0.0.59	1

Event Type distribution