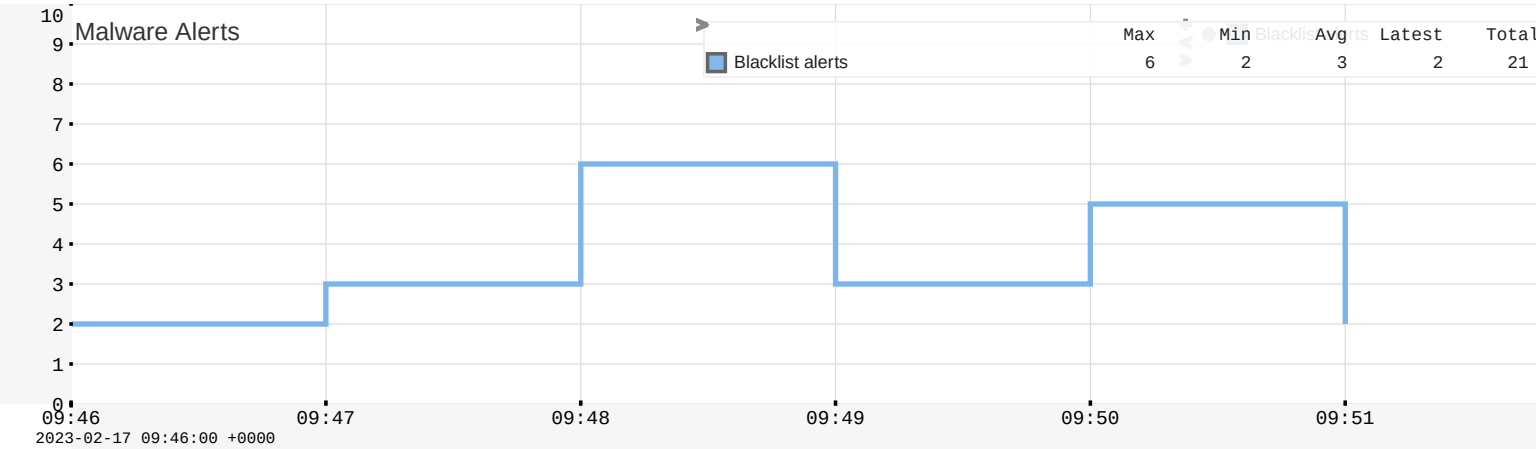
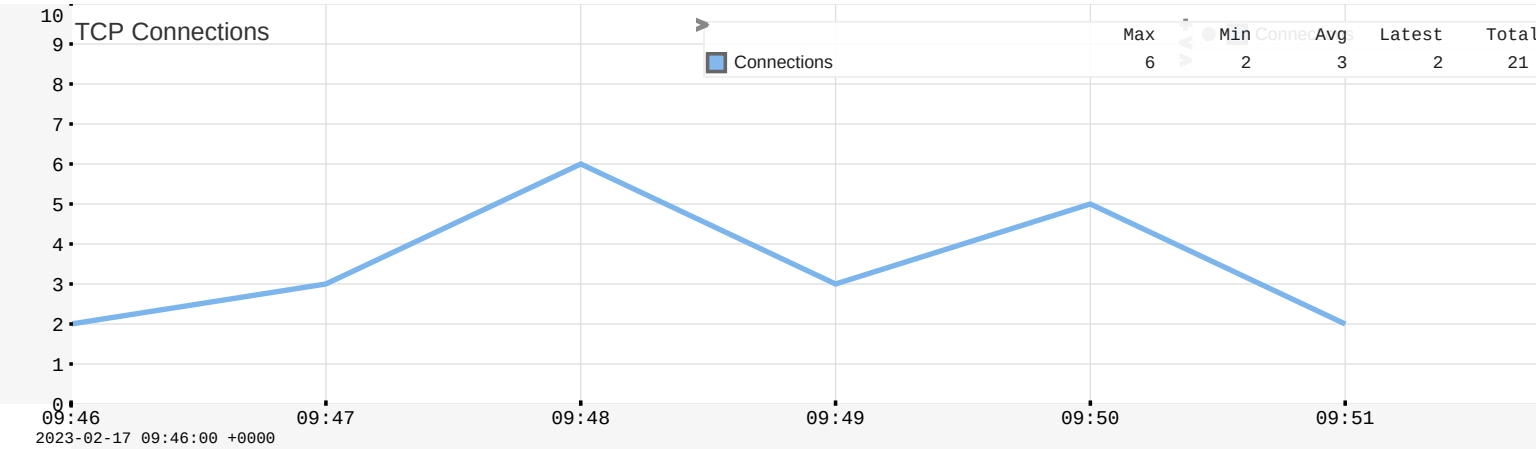
Malware alerts

Blacklist matches - show which category of blacklisted traffic was seen

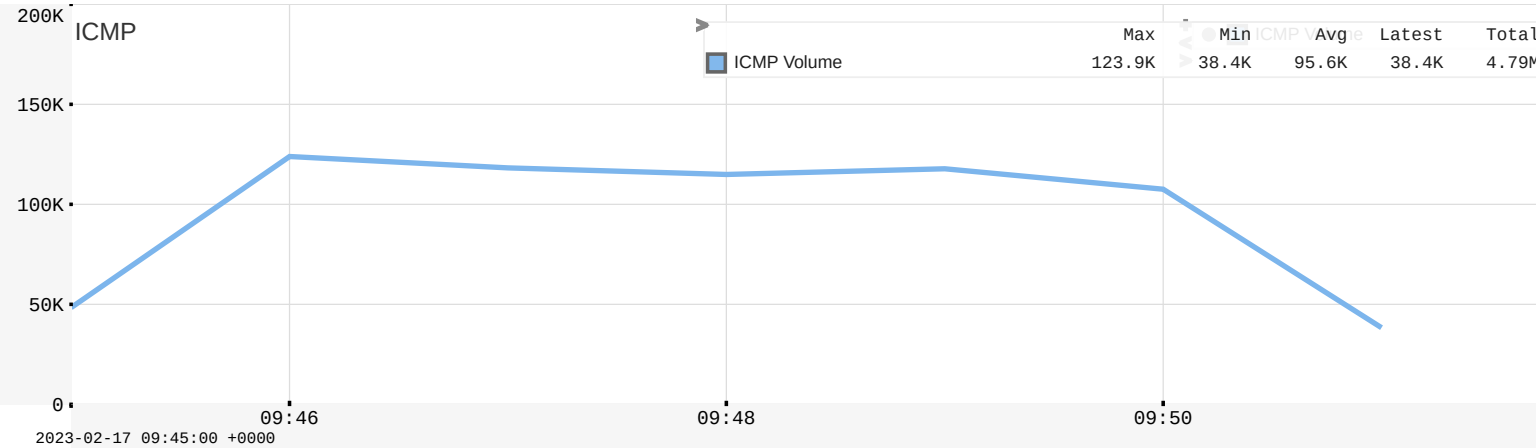


Connection activity with blacklist hits



ICMP

Activity of ICMP: can indicate port scanning, PING flood, and other attacks



Top 50 blacklisted internal hosts

Based on hitting malware,virus,phishing,spamming blacklists

Rank	Name	Volume

Top 50 blacklisted external hosts

Based on hitting malware,virus,phishing,spamming blacklists

Rank	Name	Volume

Top Alerts type

Blacklist that tgiggered alerts

Rank	Name	Volume
1	TOR-NODE	13
2	ALIENVAULT	5
3	FEODO-TRACKER-IP	1

Latest Malware Alerts
Actual alert session

Type	Fired Time	End Points	Message
ALIENVAULT	2023-02-17 09:50:12 +0000	172.22.64.123 56713 81.69.9.71 microsoft-ds	81.69.9.71 # Malicious Host CN,,39.9289016724,116.388298035
TOR-NODE	2023-02-17 09:50:05 +0000	172.26.21.2 59739 94.23.247.42 https	94.23.247.42|wien|443|80|FGHRSDV|2898120|Tor 0.4.4.5|0xFFFFFFFF Random Person <nobody AT example dot com>
ALIENVAULT	2023-02-17 09:49:46 +0000	172.21.152.251 9626 139.162.131.125 microsoft-ds	139.162.131.125 # Malicious Host DE,Frankfurt Am Main,50.1152992249,8.68229961395
TOR-NODE	2023-02-17 09:49:42 +0000	172.21.97.73 57961 83.226.156.19 microsoft-ds	83.226.156.19|karen|443|8080|FGHRSDV|6908905|Tor 0.4.2.7|karen@is-fantabulo.us
TOR-NODE	2023-02-17 09:49:30 +0000	172.29.161.233 59190 131.188.40.189 https	131.188.40.189|gabelmoo|443|80|ARSDV|7002108|Tor 0.4.4.5|4096R/261C5FBE77285F88FB0C343266C8C2D7C5AA446D Sebastian Hahn <tor@sebastianhahn.net> - 12NbRAjAG5U3LLWETSF7fSTcdaz32Mu5CN
TOR-NODE	2023-02-17 09:49:17 +0000	172.26.21.2 59719 66.206.0.82 9001	66.206.0.82|8rijgto8|9001|9030|FGHRSDV|47669713|Tor 0.3.5.7|
TOR-NODE	2023-02-17 09:49:02 +0000	172.26.21.2 59712 51.15.185.201 https	51.15.185.201|PoochySloochy|443|80|FGHRSDV|29396692|Tor 0.3.5.7|
ALIENVAULT	2023-02-17 09:48:41 +0000	172.27.18.93 56286 220.132.94.153 microsoft-ds	220.132.94.153 # Malicious Host TW,Taipei,25.0478000641,121.531799316
TOR-NODE	2023-02-17 09:48:13 +0000	172.26.21.2 59698 185.32.222.237 9443	185.32.222.237|bauruine|9443|8081|FGHRSDV|3839137|Tor 0.4.4.5|Bauruine <torcontact aatt tuxli.ch> - 1CVkdZfRGWXETqVu8ctEKKMPC8Xj2Xnqcp
FEODO-TRACKER-IP	2023-02-17 09:48:06 +0000	172.27.18.69 58790 100.14.117.137 microsoft-ds	100.14.117.137
TOR-NODE	2023-02-17 09:47:52 +0000	172.26.21.2 59690 95.153.31.26 https	95.153.31.26|Mack|443|80|FGHRSDV|6322246|Tor 0.3.5.10|
TOR-NODE	2023-02-17 09:47:34 +0000	172.26.21.2 59685 5.9.121.207 https	5.9.121.207|ENiGMA|443|80|FGHRSDV|1947656|Tor 0.4.4.6|enigma[aet]s0ny(d0t)net
TOR-NODE	2023-02-17 09:47:33 +0000	172.26.21.2 59686 158.58.173.78 https	158.58.173.78|duke|443|80|FGRSDV|194582|Tor 0.4.3.5|
TOR-NODE	2023-02-17 09:47:33 +0000	172.27.56.64 53038 199.58.81.140 https	199.58.81.140|longclaw|443|80|ARSDV|1231394|Tor 0.4.4.6|Riseup Networks <collective at riseup dot net> - 1nNzekuHGGzBYRzyjfjFEfeisNvxkn4RT
TOR-NODE	2023-02-17 09:47:30 +0000	172.26.21.2 59683 51.158.170.28 https	51.158.170.28|KienjochFR|443|9030|FGHRSDV|4305674|Tor 0.3.5.10|<KienjochFRInfo> contact(at)torrelay(dot)de
TOR-NODE	2023-02-17 09:47:10 +0000	172.26.21.2 59673 45.125.65.45 https	45.125.65.45|katharina|443|80|EFGHRSDV|3610939|Tor 0.3.5.10|
ALIENVAULT	2023-02-17 09:46:37 +0000	172.27.10.218 53909 162.62.26.10 microsoft-ds	162.62.26.10 # Malicious Host RU,,55.7386016846,37.6068000793
TOR-NODE	2023-02-17 09:46:28 +0000	172.26.21.2 59655 46.4.78.148 9001	46.4.78.148|buttercup|9001|9030|FGHRSDV|367200|Tor 0.3.5.12|https://schulz.com.de/contact/?addr=buttercup
TOR-NODE	2023-02-17 09:46:09 +0000	172.26.21.2 59645 62.210.105.46 9201	62.210.105.46|Assange008fr2|9201|9211|FGHRSDV|713043|Tor 0.4.4.6|BMTY90VKYRQPUJZOTH[@]Safe-mail.net
ALIENVAULT	2023-02-17 09:45:29 +0000	172.21.97.79 52866 180.136.133.184 microsoft-ds	180.136.133.184 # Malicious Host CN,Nanning,22.8166999817,108.316703796
ALIENVAULT	2023-02-17 09:45:01 +0000	172.22.65.32 64593 128.14.209.238 microsoft-ds	128.14.209.238 # Malicious Host US,Los Angeles,34.0728988647,-118.260597229