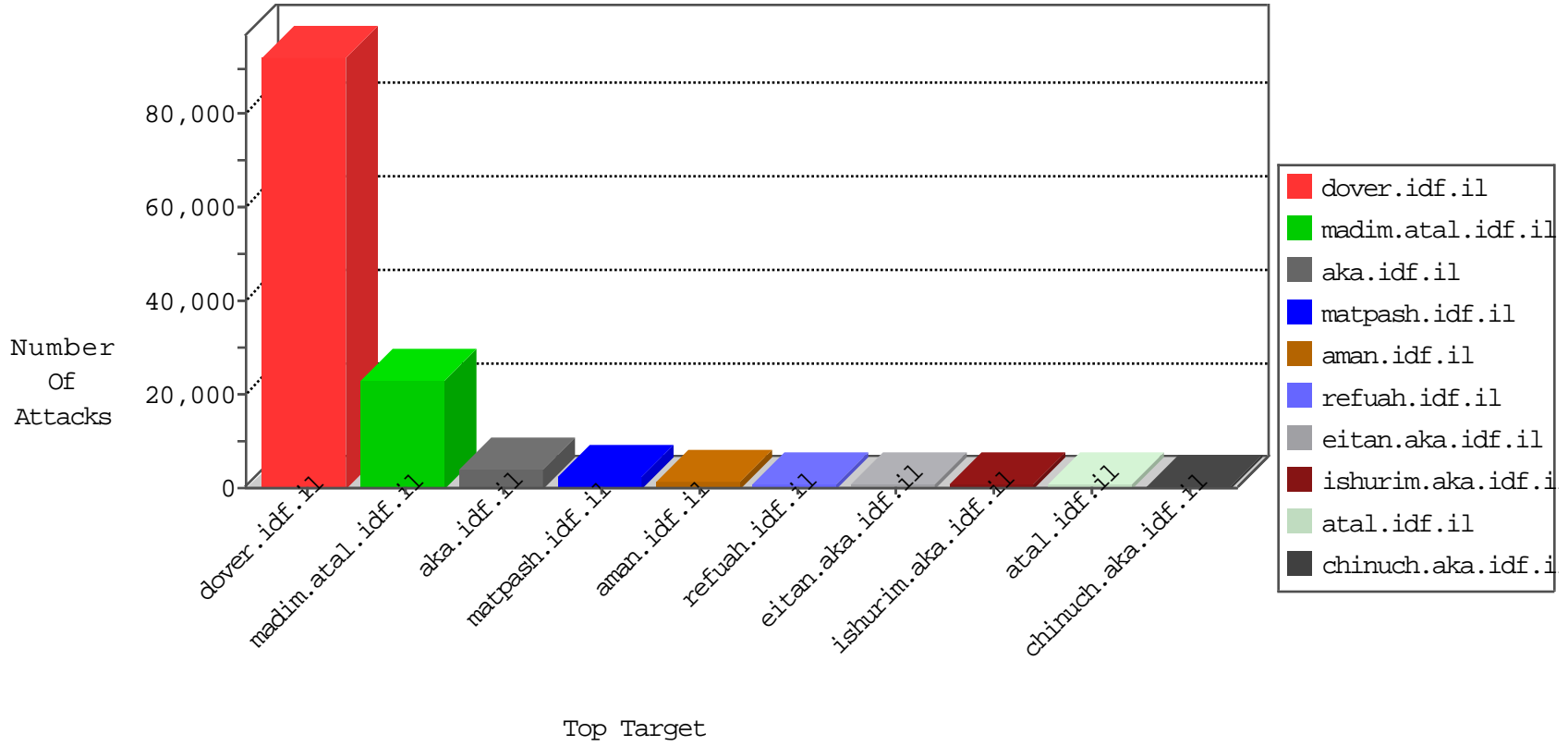


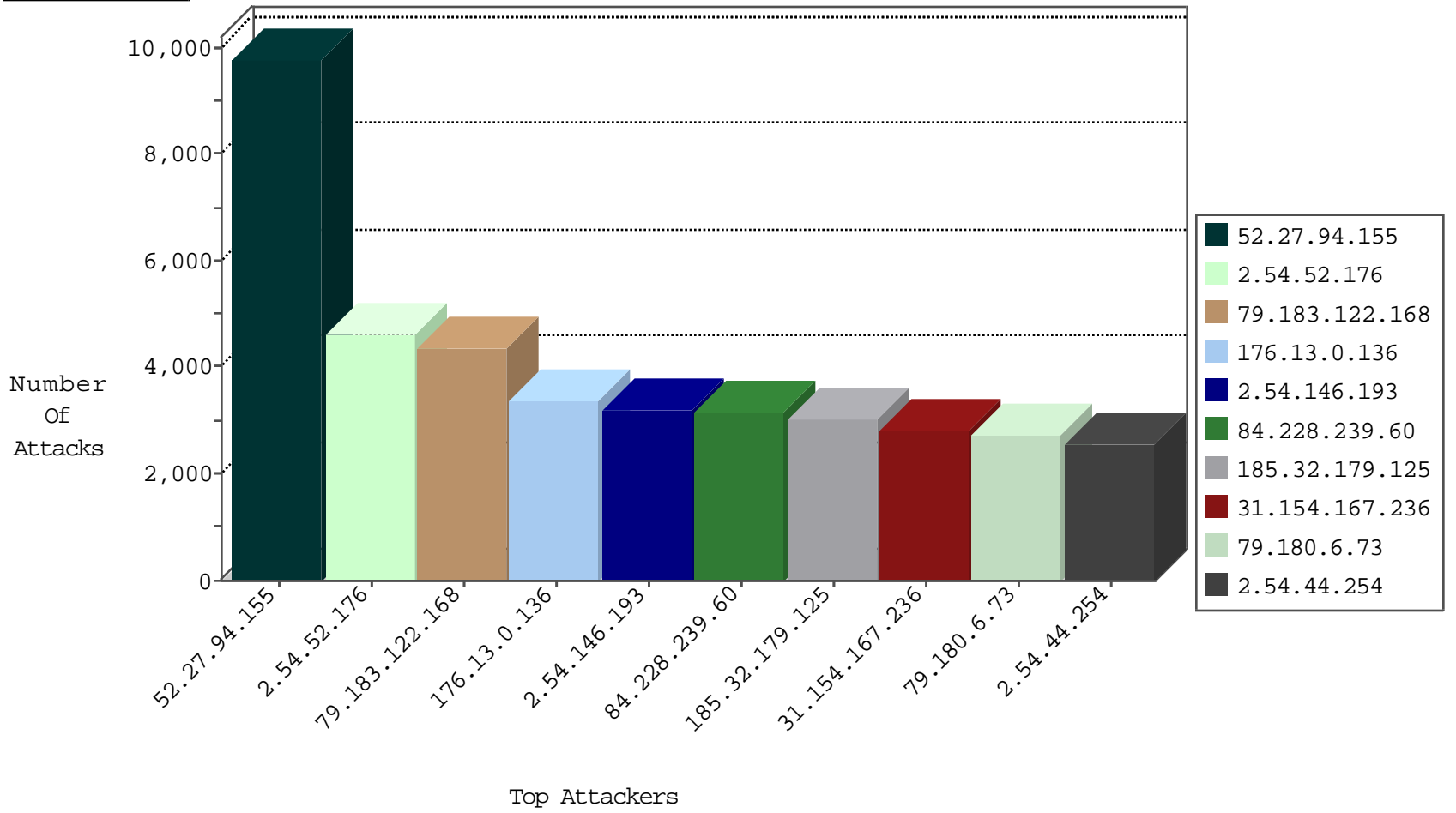
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	29666
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	18964
45.101.195.88		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14720
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11808
198.58.102.95	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3005
66.249.81.212	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2768
87.68.67.177	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2746
31.154.25.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2602
54.187.55.213	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1638
188.247.77.221	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1127
82.166.23.32	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1035
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	709
46.117.100.187	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	644
109.64.3.35	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	576
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	546
79.180.200.165	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	488
79.182.25.227	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	486
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	450
79.179.10.97	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	445
79.182.173.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	437
77.125.151.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	357
79.180.189.232	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	356
85.65.194.161	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	300
84.229.78.90	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	299
5.22.135.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	291
5.29.63.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	285
66.102.7.233	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	263
93.172.171.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	262
5.102.254.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	236
5.29.180.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	231
5.29.50.107	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
79.177.39.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	190
95.86.64.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	186
109.64.129.238	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	181
5.28.173.198	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	176
79.182.30.112	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	169
79.177.191.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
79.182.168.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
213.151.52.131	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	149
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	148
79.179.149.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
84.108.211.106	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
46.120.17.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
213.8.81.94	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	130
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
46.120.198.214	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	128
149.78.59.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
84.108.105.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
197.205.106.164	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Product	dest-reset	118

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.180.6.73	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	211
82.166.23.32	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	72
194.90.66.9	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	61
89.139.63.235	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	12
46.120.143.209	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	10
84.111.155.234	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	10
5.29.203.239	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	10
186.26.115.4	Costa Rica	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	7
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
212.34.11.47	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
85.65.127.14	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
84.228.110.135	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
31.154.92.164	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
46.19.85.127	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
46.120.126.140	Israel	147.237.76.30	himush.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
2.54.36.70	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
46.19.85.209	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
212.179.148.59	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.97	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
5.22.135.177	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
5.29.173.253	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
211.59.8.170	Korea, Republic of	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
46.19.85.70	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
79.178.145.230	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.18	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
77.127.66.119	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
175.143.19.180	Malaysia	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
84.109.113.39	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
80.234.11.158	Russian Federation	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
79.176.177.210	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
111.68.38.134	Philippines	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
46.19.85.11	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
194.90.66.9	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
176.106.226.5	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
37.78.244.169	Russian Federation	147.237.77.216	dover.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	2
89.138.204.218	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.19.85.21	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
104.162.155.116		147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
84.229.32.107	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
62.0.105.133	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
201.167.84.39	Mexico	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
105.155.148.35	Morocco	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
195.244.23.42	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.159.170.19	Russian Federation	147.237.77.170	maarachot.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	2
176.106.44.50	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.19.86.201	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
109.67.189.86	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
65.36.76.195	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
212.199.130.50	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	73
176.13.17.93	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
89.66.196.175	Poland	147.237.77.216	dover.idf.il	SERVER-WEBAPP yabb access	6
89.66.196.175	Poland	147.237.77.176	matpash.idf.il	SERVER-WEBAPP yabb access	4
176.12.149.101	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.83.137	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
122.10.102.45	Hong Kong	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.137	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
149.78.154.69	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.148	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
176.13.1.174	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
122.10.102.47	Hong Kong	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
193.105.134.220	Sweden	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
122.10.102.45	Hong Kong	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
122.10.102.47	Hong Kong	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
89.66.196.175	Poland	147.237.77.216	dover.idf.il	SERVER-WEBAPP modules.php access	2
122.10.102.47	Hong Kong	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
52.76.73.144	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	2
189.124.0.201	Brazil	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
89.66.196.175	Poland	147.237.77.176	matpash.idf.il	SERVER-WEBAPP modules.php access	2
122.10.102.47	Hong Kong	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
66.249.78.130	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
218.65.30.107	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
222.186.21.180	China	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
182.243.85.138	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
119.235.50.45	India	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
182.243.85.138	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
122.10.102.47	Hong Kong	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
62.90.210.236	Israel	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
122.10.102.49	Hong Kong	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
85.64.64.105	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
46.60.54.88	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
122.10.102.45	Hong Kong	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
69.64.46.86	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	2
94.102.56.130	Netherlands	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
182.243.85.138	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.178.2.23	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
123.151.149.222	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.252.216.200	Vietnam	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
52.76.73.144	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 4096	1
122.10.102.46	Hong Kong	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
208.68.36.51	United States	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.32.5	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.20		147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
189.124.0.201	Brazil	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.118	Switzerland	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
122.10.102.47	Hong Kong	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
218.65.30.107	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
52.27.94.155	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9772
2.54.52.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4622
79.183.122.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4376
84.228.239.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3152
31.154.167.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2806
79.180.6.73	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2530
105.98.60.170	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1886
95.86.109.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1848
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1519
82.145.223.69	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1363
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1224
8.37.224.183	Anonymous Proxy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1013
70.39.185.213	Satellite Provider	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	971
149.88.140.2	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	946
95.86.108.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	895
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	892
212.179.71.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	887
82.145.222.188	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	817
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	728
54.187.55.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	726
31.13.164.132	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	588
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	533
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	495
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	494
2.54.166.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	490
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	478
208.109.97.62	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	477
212.150.112.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	473
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	464
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	462
8.39.233.9	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	461
46.19.86.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	459
132.76.50.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	424
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	400
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	394
41.68.241.123	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	373
208.109.97.62	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	367
24.234.188.79	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	352
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	304
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	290
66.87.78.126	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	279
46.19.86.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	266
205.203.99.41	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	238
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	230
37.231.131.252	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	221
213.151.36.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	215
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	214
157.55.39.124	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	214
157.55.39.237	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	210
197.205.106.164	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	203

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.13.0.136	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.0.136	Block	3366
2.54.146.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3201
185.32.179.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3048
2.54.44.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2537
109.253.156.202	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.156.202	Block	1842
46.19.86.242	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.242	Block	1439
80.246.139.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1093
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	960
77.127.101.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	960
185.32.179.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	588
109.241.134.160	Poland	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	588
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.240	Block	552
2.54.184.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	527
2.54.38.216	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.38.216	Block	480
185.32.179.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	412
37.142.64.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	372
37.26.147.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	318
80.246.136.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	276
185.32.179.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	270
84.108.235.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	204
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	162
185.32.179.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	126
84.228.143.132	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	114
89.66.196.175	Poland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 89.66.196.175	Block	114
46.19.86.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	108
185.32.179.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
185.32.179.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	90
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	84
81.218.97.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	78
114.77.15.216	Australia	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 114.77.15.216	Block	66
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	66
5.29.119.75	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 5.29.119.75	Block	66
192.115.248.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	66
185.32.179.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
212.150.209.205	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.150.209.205	Block	60
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	60
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	60
66.249.64.207	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	48
81.218.70.243	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	48
185.32.179.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
46.120.84.148	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.120.84.148	Block	48
212.179.21.194	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	48
89.66.196.175	Poland	147.237.77.176	matpash.idf.il	PHP Attempt	Block	48
66.249.64.154	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	36
79.176.102.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	36
2.54.49.88	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.49.88	Block	36
66.249.64.212	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	36
46.116.93.192	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	36
79.179.49.174	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	36
66.249.64.202	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	36