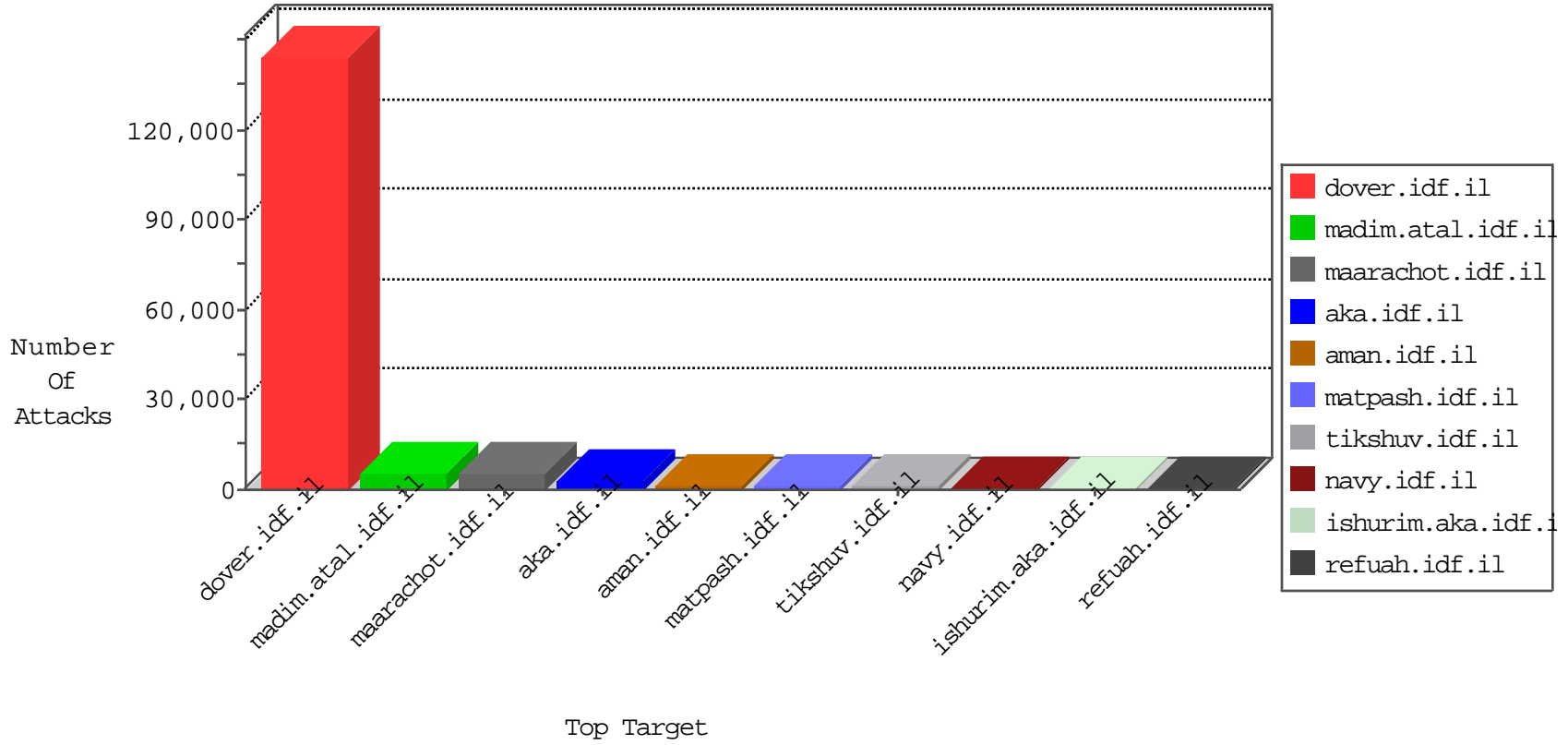


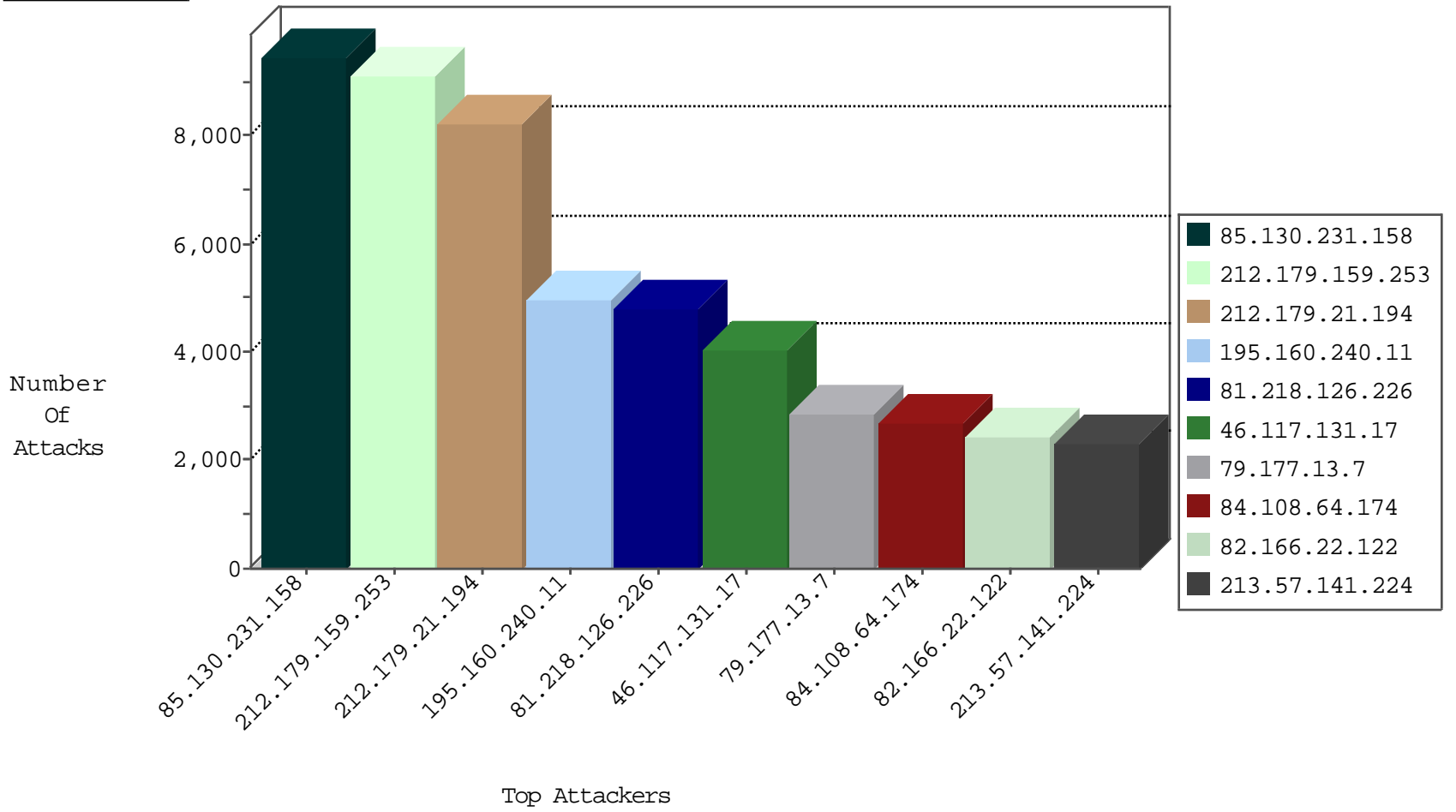
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
46.197.71.92	Turkey	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	39299
81.218.126.226	Israel	147.237.77.170	maarachot.idf.il	TCP Scan (vertical)	drop	25057
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	24292
66.249.93.172	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3913
195.34.150.18	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2957
77.127.204.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	2703
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2594
5.29.18.244	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	730
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	728
79.176.125.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	721
82.145.222.176	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	507
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	495
79.181.152.12	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	401
37.46.39.56	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	386
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	385
213.151.53.161	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	350
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	318
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	296
46.197.71.92	Turkey	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	243
109.253.147.152	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	239
188.169.78.111	Georgia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	236
5.29.88.202	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	233
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	230
37.46.39.95	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	218
85.65.91.182	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
46.197.71.92	Turkey	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	187
83.130.101.135	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	177
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
77.125.10.28	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
84.111.36.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
109.66.1.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
220.181.108.161	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	162
79.178.112.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	159
212.117.143.250	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
46.197.71.92	Turkey	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-lgn	dest-reset	142
109.253.149.234	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
82.166.22.125	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	133
109.64.139.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
176.228.136.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
5.90.107.60	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	126
85.250.113.163	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
79.180.201.223	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
77.126.151.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
77.127.202.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
46.117.117.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
77.125.255.136	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
85.64.18.164	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
185.32.178.218	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	760
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	471
77.127.204.103	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	198
61.145.194.228	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	34
198.100.144.75	Canada	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	20
104.155.201.192		147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
104.155.201.192		147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
104.155.201.192		147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
104.155.201.192		147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
109.67.186.201	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
46.19.85.53	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	9
109.64.105.149	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
194.90.153.133	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
85.64.144.165	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
81.218.126.226	Israel	147.237.77.170	maarachot.idf.il	0234: HTTP: Nimda / Code Red / Code Blue Attack	Block	6
84.109.184.181	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
66.240.192.138	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	5
5.29.227.76	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
62.219.13.180	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.178.112.170	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
218.77.79.43	China	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	4
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	4
218.77.79.43	China	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	4
77.126.0.112	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	4
62.219.183.178	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
218.77.79.43	China	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	4
80.178.138.130	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	4
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	4
62.90.35.105	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
82.166.22.122	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
188.138.9.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	4
218.77.79.43	China	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	4
183.171.164.255	Malaysia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	3
212.143.56.182	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.240.192.138	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	3
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	3
218.77.79.43	China	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
218.77.79.43	China	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	3
79.177.6.88	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3

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	90
105.109.96.66	Algeria	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	11
89.234.68.89	Ireland	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	10
105.109.96.66	Algeria	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	10
89.234.68.87	Ireland	147.237.72.156	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	8
27.75.97.63	Vietnam	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	7
82.166.22.122	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	7
88.245.66.151	Turkey	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
27.75.97.63	Vietnam	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	6
89.234.68.86	Ireland	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
43.255.188.131	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	4
43.255.188.131	Japan	147.237.76.147	chimuch.aka.idf.il	ET SCAN Potential SSH Scan	4
66.249.93.222	United States	147.237.76.147	chimuch.aka.idf.il	ET SCAN NMAP -sA (2)	4
43.255.188.131	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.131	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	3
43.255.188.132	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.132	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.131	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	3
46.19.86.61	Israel	147.237.76.31	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
43.255.188.131	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.131	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.131	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.131	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
50.57.139.99	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
84.95.58.132	Israel	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
109.253.149.234	Israel	147.237.77.216	dover.idf.il	INDICATOR-SCAN myscan	2
176.12.150.79	Israel	147.237.77.216	dover.idf.il	GPL SCAN myscan	2
218.208.35.222	Malaysia	147.237.77.216	dover.idf.il	SQL Injection - Union Select (POST)	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.131	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
199.203.59.121	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
94.230.86.222	Israel	147.237.77.216	dover.idf.il	GPL SCAN myscan	2
66.249.79.25	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
104.155.201.192		147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
61.183.128.6	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.131	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.132	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.69.92	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
85.130.231.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9465
212.179.159.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9097
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7913
195.160.240.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4951
46.117.131.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4047
79.177.13.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2835
84.108.64.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2683
82.166.22.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2356
213.57.141.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2292
79.177.179.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1681
2.54.162.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1309
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1170
80.254.147.148	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1142
2.54.1.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1012
46.19.85.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	945
109.160.182.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	932
2.54.24.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	919
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	870
105.109.96.66	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	831
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	804
80.94.146.18	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	792
2.54.9.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	791
79.176.56.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	774
82.80.89.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	749
82.166.117.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	721
79.176.152.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	684
46.197.71.92	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	641
168.235.197.139		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	637
2.54.19.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	590
85.64.114.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	551
95.86.71.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	545
5.102.254.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	534
109.186.0.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	528
41.69.147.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	513
37.26.146.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	493
2.52.47.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	492
2.52.38.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	485
37.26.147.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	474
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	472
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	470
2.54.150.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	468
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	465
2.54.50.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	463
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	463
89.139.15.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	459
2.54.2.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	457
95.86.67.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	444
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	441
2.54.151.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	440
2.54.19.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	438

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.138.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	777
2.54.24.246	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.24.246	Block	382
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.150	Block	369
105.109.96.66	Algeria	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	355
2.54.37.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	323
176.12.149.191	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.149.191	Block	292
87.68.254.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	284
176.12.150.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	248
109.253.141.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.141.199	Block	223
37.26.147.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	197
176.12.143.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	195
176.12.138.209	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.138.209	Block	194
109.253.135.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	186
176.12.150.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	171
109.253.156.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	171
2.54.12.29	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.12.29	Block	162
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	143
176.12.138.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	123
176.13.15.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	91
95.35.50.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
109.253.144.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	62
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	60
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	60
2.54.129.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
2.54.37.36	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.37.36	Block	48
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	45
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	43
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	42
176.13.13.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	40
105.109.96.66	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.109.96.66	Block	38
85.64.251.100	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	36
176.12.146.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	35
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	29
217.132.219.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	24
105.109.96.66	Algeria	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	23
46.19.85.220	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.220	Block	18
46.117.30.165	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.30.165	Block	16
79.181.155.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
31.154.148.112	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	8
188.120.148.188	Israel	147.237.72.156	anan.idf.il	Suspicious Response Code	Block	8
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	7
81.218.76.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc	Block	7
2.54.190.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
85.64.202.120	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
81.218.76.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6