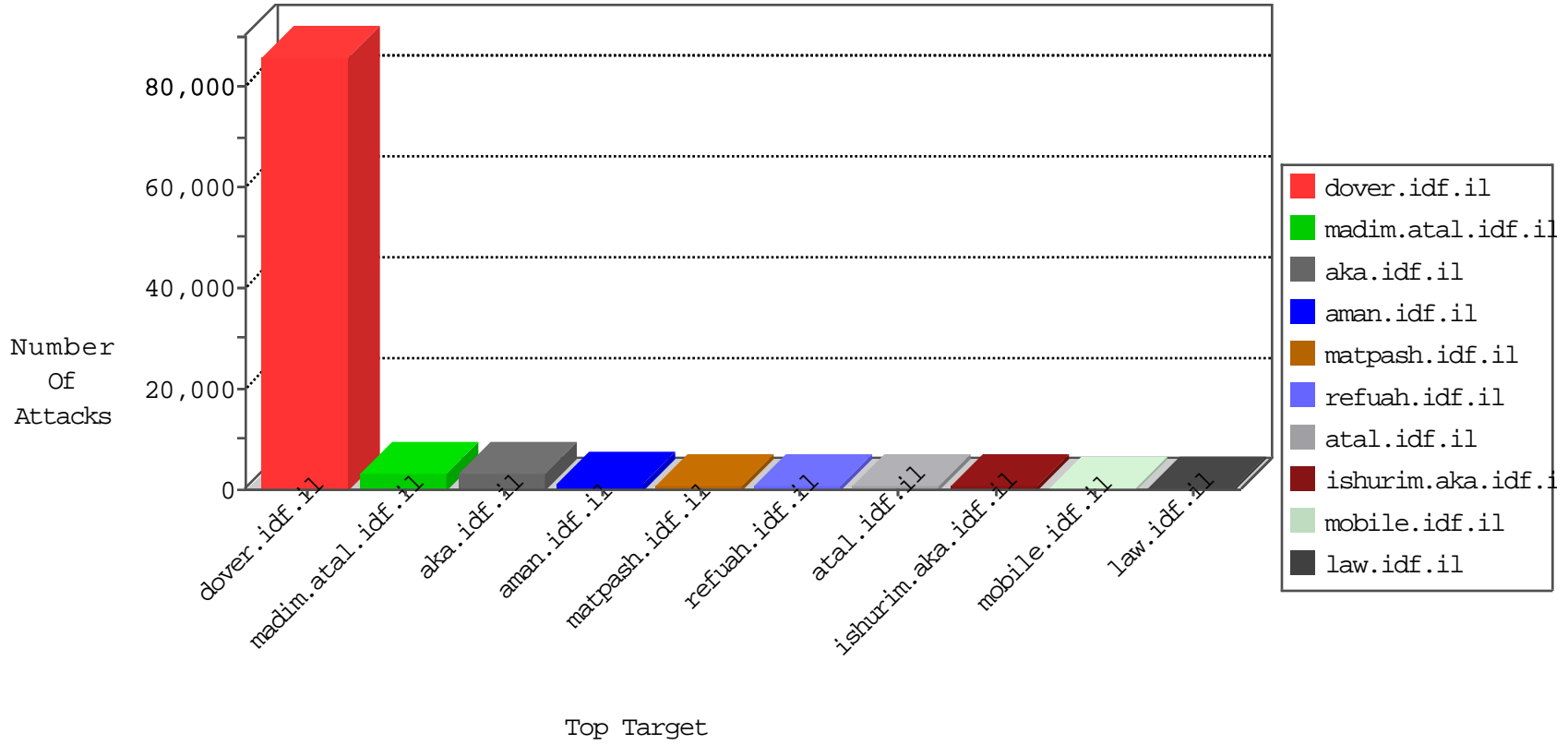


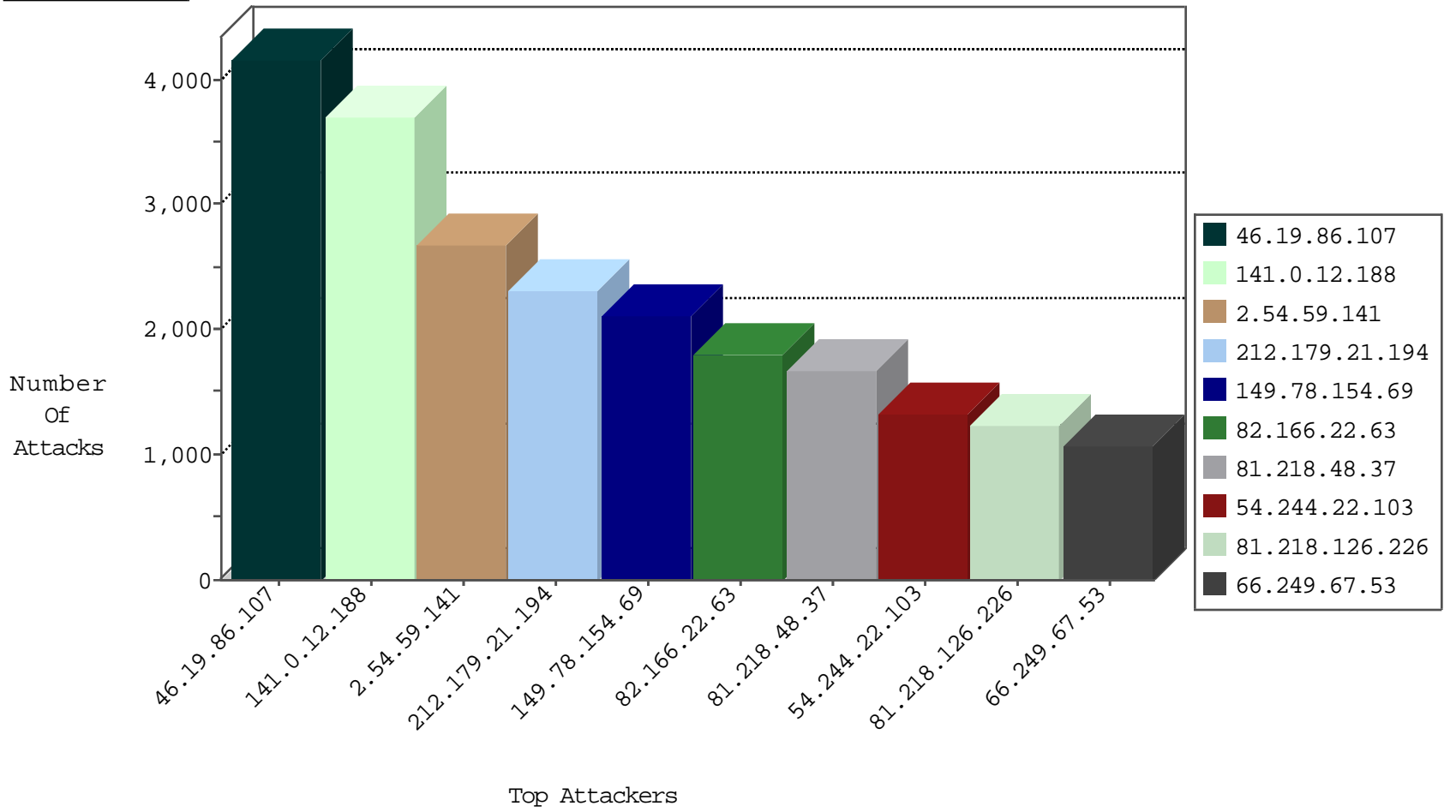
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
82.95.74.122	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8831
31.168.84.89	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6253
54.244.22.103	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5583
66.249.83.158	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3214
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3185
109.186.103.143	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2951
109.186.15.249	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2567
194.90.117.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2510
141.0.12.188	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1151
198.52.155.201	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1020
85.250.219.73	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	981
84.109.235.250	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	649
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	634
77.127.204.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	632
149.88.29.215	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	599
213.8.22.240	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	515
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	485
46.120.42.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	467
66.249.88.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	465
84.228.227.163	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	464
109.160.187.17	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	455
149.78.58.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	411
77.126.167.252	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	367
46.120.17.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	365
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	355
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	315
109.67.169.78	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	306
89.138.55.36	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	293
46.117.192.36	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	288
79.181.198.29	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	279
95.86.74.83	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	268
149.78.180.188	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	266
79.177.107.220	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	249
5.29.40.8	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
46.120.31.40	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	235
46.19.86.235	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	233
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	203
212.235.8.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	201
5.29.50.110	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
79.176.165.87	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
46.117.174.179	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
77.126.225.225	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
79.180.189.7	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
46.121.102.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
99.46.140.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	162
2.52.28.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
149.78.44.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	159
87.69.2.131	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	143
185.32.178.78	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	139

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.127.204.103	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	56
115.219.24.130	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	34
79.178.3.191	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
24.171.101.99	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
37.142.137.219	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
207.232.12.216	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
213.139.53.17	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
99.109.127.146	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
5.22.129.206	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.65.150.219	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
200.129.187.61	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.178.129.162	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.153	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.95.1.230	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.197	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
89.138.54.235	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.80	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.182.101.11	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.65.124.140	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
109.186.170.192	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
87.68.153.166	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.120.145.62	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.178.26.50	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
192.118.78.57	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
132.70.66.11	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.250.162.82	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.3	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.207	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.102	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.57.174.130	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.183.10.68	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.178.3.191	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
37.26.146.170	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.95.210.120	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.64.80.25	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.138.54.235	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.64.2.26	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.51	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
94.226.191.102	Belgium	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
78.94.83.192	Germany	147.237.77.233	atal.idf.il	C1000106: HTTP: majestic bot	Block	1
85.64.207.93	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.121.94.141	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.207	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
82.102.169.113	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.127.181.150	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
37.26.148.199	Israel	147.237.76.39	mobile.meitav.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
2.54.181.143	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.109.232.145	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
73.170.16.243	United States	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	23
82.166.22.63	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	9
54.209.60.63	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	8
66.249.67.59	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	8
212.38.162.92	United Kingdom	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	3
188.161.183.103	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	3
43.255.188.132	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	3
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
185.12.94.56	Russian Federation	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
198.52.155.201	United States	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
43.255.188.135	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
41.218.183.95	Egypt	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
61.240.144.67	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.132	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.130	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.206	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.135	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
5.9.121.120	Germany	147.237.77.216	dover.idf.il	ET WEB_SERVER Poison Null Byte	2
43.255.188.132	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
198.52.155.201	United States	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
43.255.188.132	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.226	www.chamatz.aka.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
43.255.188.132	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	2
61.183.128.6	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
43.255.188.135	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
178.89.191.77	Kazakhstan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.7	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
192.3.108.133	United States	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
119.97.231.102	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
43.255.188.132	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
79.191.42.147	Poland	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
2.54.141.76	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.107	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4162
141.0.12.188	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3669
2.54.59.141	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2612
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2171
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2108
82.166.22.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1772
81.218.48.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1649
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	883
66.249.67.59	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	671
66.249.67.65	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	660
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	648
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	643
66.249.67.53	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	640
87.68.246.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	613
81.218.126.226	Israel	147.237.72.166	aka.idf.il	SQL injection detected in URL: 'CONCAT'	SQL Injection	monitor	613
164.138.114.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	610
66.249.83.158	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	601
95.86.112.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	597
46.210.132.141	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	575
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	571
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	568
66.249.83.161	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	564
212.179.180.30	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	562
66.249.83.155	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	557
107.77.100.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	532
77.127.188.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	480
2.54.41.188	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	454
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	433
54.244.22.103	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	425
54.244.22.103	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	417
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	411
109.186.0.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	387
213.57.41.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	369
66.249.81.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	362
54.187.55.213	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	354
198.239.77.118	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	327
66.249.81.218	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	324
66.87.82.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	320
66.249.81.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	319
66.102.6.171	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	298
5.255.253.33	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	290
2.54.29.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	280
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	277
79.180.145.215	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	274
66.102.6.163	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	265
95.86.84.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	265
37.236.136.12	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	264
66.102.6.167	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	263
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	263
172.56.26.12	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	262

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
94.230.86.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	861
46.117.192.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	397
2.54.179.89	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.179.89	Block	380
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	329
2.54.50.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	220
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	207
46.19.85.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	185
2.54.44.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	122
176.12.136.188	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	121
176.13.1.131	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.1.131	Block	114
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	93
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	88
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	79
176.13.14.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	78
2.54.185.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
80.246.136.43	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.43	Block	62
176.12.144.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	61
85.64.27.57	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.27.57	Block	48
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	31
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	30
2.54.0.149	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.0.149	Block	29
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	28
37.142.183.64	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
81.218.33.77	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
2.52.32.39	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.32.39	Block	18
149.88.181.92	United States	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 149.88.181.92	Block	16
80.227.88.41	United Arab Emirates	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	15
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	14
46.19.85.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	11
212.76.108.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
200.53.156.246	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	10
46.19.85.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
80.179.197.12	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	10
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	10
85.65.124.140	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 85.65.124.140	Block	7
176.12.136.188	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
2.54.142.221	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	6
176.12.136.188	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	6
207.46.13.28	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
213.251.182.115	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.251.182.115	Block	5
85.65.47.80	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	5
94.230.86.132	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	5
85.64.109.141	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
91.200.12.56	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	4
46.19.85.98	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	4
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	4
46.116.134.106	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.116.134.106	None	4
2.54.48.12	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	4