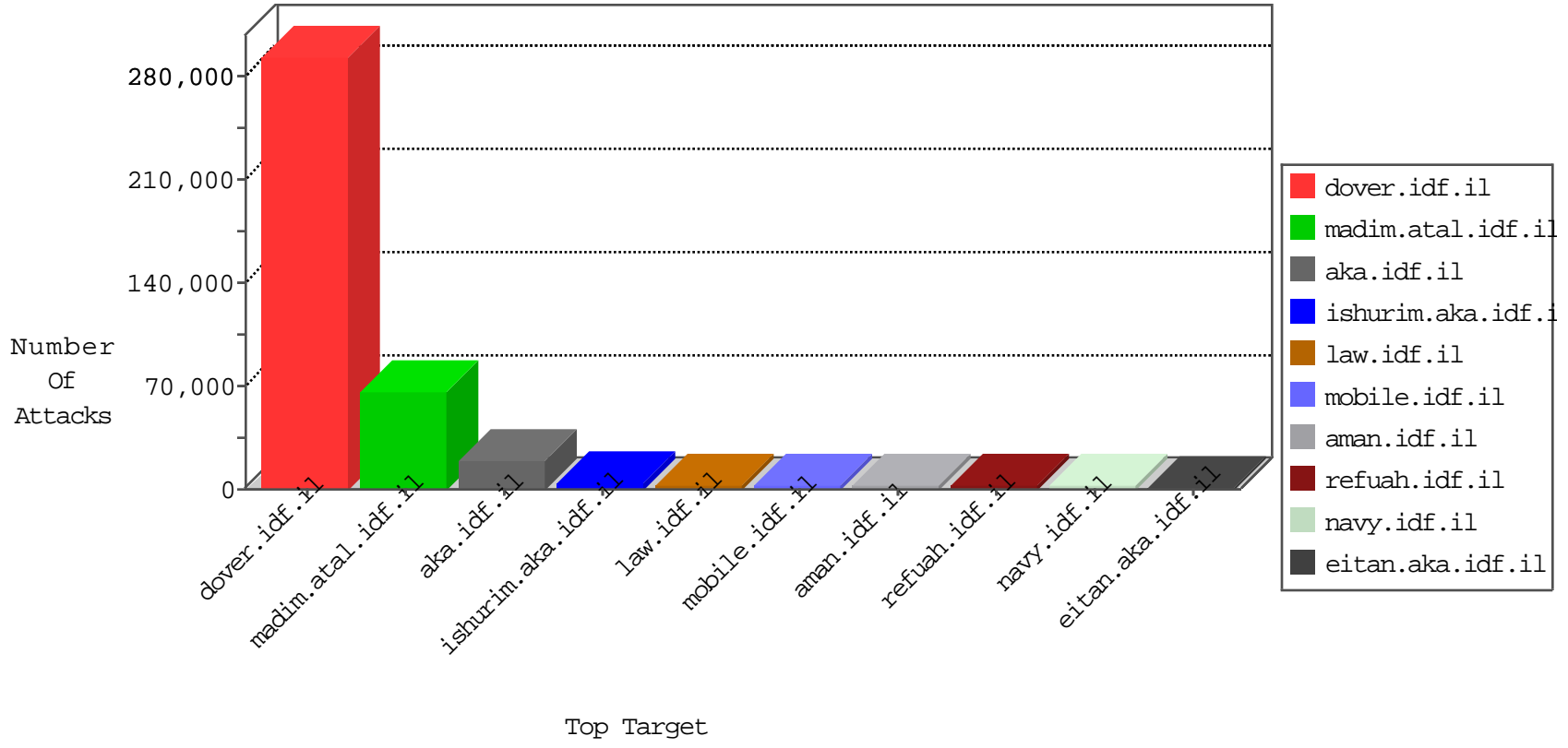


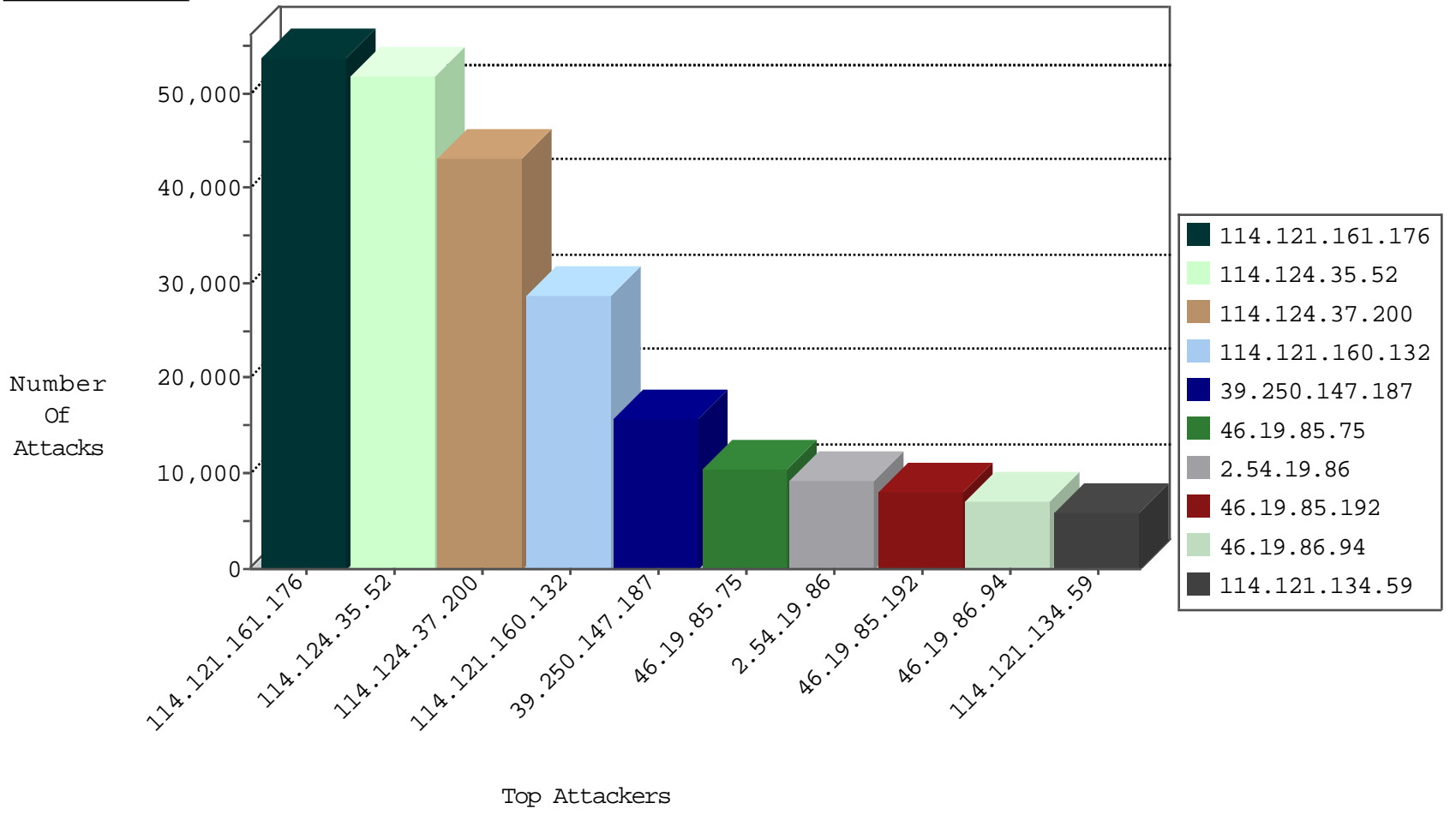
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.229.164.99	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40996
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	25661
66.249.67.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7359
178.214.88.189	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6500
66.249.67.59	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4271
66.249.67.50	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3548
109.67.250.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3472
74.80.213.22	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2943
101.188.57.201	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2927
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2568
66.249.64.146	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2542
66.249.64.3	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1450
166.137.126.33	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1171
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1142
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	900
66.249.67.12	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	715
82.80.17.247	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	448
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	299
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	296
66.249.67.56	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	226
176.106.227.53	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	182
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	179
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	149
46.19.86.58	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	145
80.246.139.52	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	145
2.54.43.169	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	139
46.19.86.82	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	135
37.26.148.203	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	133
2.54.168.202	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	129
46.19.85.81	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	106
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
37.26.148.135	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	89
46.19.86.169	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	83
37.26.146.191	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	82
185.32.179.16	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	78
37.26.149.215	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	75
91.228.248.251	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	69
2.54.169.47	Israel	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	66
46.19.86.197	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	64
80.246.139.21	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	63
82.80.17.247	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
46.19.85.113	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	61
185.13.192.230	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	59
80.179.31.27	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	57
37.26.148.136	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	53
46.19.85.132	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	52
66.249.67.125	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	50
37.26.147.177	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	48
46.19.86.217	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	48
46.19.86.191	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	46

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.135.111.85	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
79.178.222.86	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
222.84.5.232	China	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
198.143.164.7	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
94.245.88.135	United Kingdom	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
76.74.252.117	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
216.201.148.210	United States	147.237.77.233	atal.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	4
108.168.219.174	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
77.242.124.2	Netherlands	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
79.182.141.240	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
197.246.244.17	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
82.166.146.134	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.181.22.28	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
192.198.151.36	Europe	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
103.21.58.191	India	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
82.208.46.148	Czech Republic	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
84.228.102.24	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
212.179.213.153	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
213.151.36.98	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
169.240.96.42	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.116.206.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
198.20.69.74	United States	147.237.8.28	e.mobile-ks.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
192.198.151.44	Europe	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
23.91.127.130	United States	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
212.179.93.114	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.177.214.116	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
178.219.244.158	Ukraine	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
23.91.127.130	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
79.183.224.154	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
72.64.157.108	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
166.62.93.125	United States	147.237.77.176	matpash.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
89.36.197.64	Romania	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
185.24.76.131	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
37.59.60.67	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
198.20.69.74	United States	147.237.8.24	e.lifestyle.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
91.121.169.194	France	147.237.76.200	eitan.aka.idf.il	C1000106: HTTP: majestic bot	Block	1
207.67.117.12	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
77.232.140.250	Russian Federation	147.237.77.176	matpash.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
5.172.153.183	United Kingdom	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
177.85.66.25	Brazil	147.237.77.74	law.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
212.150.245.250	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
79.182.133.205	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
62.90.255.56	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
217.118.95.82	Russian Federation	147.237.77.74	law.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
82.208.46.148	Czech Republic	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
198.20.69.74	United States	147.237.77.121	e.navy.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
178.121.156.237	Belarus	147.237.77.74	law.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	105
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	59
82.208.46.148	147.237.77.216	Czech Republic	dover.idf.il	SQL Injection - Select From	16
62.210.226.9	147.237.77.216	France	dover.idf.il	SQL Injection - Select From	13
108.168.219.174	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	12
216.201.148.210	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
37.26.148.226	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
167.114.210.166	147.237.77.216	Canada	dover.idf.il	Tehila - Perl LWP with fake user agent	8
198.143.164.7	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
80.246.136.84	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
76.74.252.117	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
103.21.58.191	147.237.77.74	India	law.idf.il	SQL Injection - Select From	5
23.91.127.130	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	5
216.27.29.16	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	5
77.242.124.2	147.237.72.166	Netherlands	aka.idf.il	SQL Injection - Select From	4
94.245.88.135	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	4
66.249.67.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
159.8.28.242	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
195.74.38.14	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	3
52.16.5.197	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	3
66.249.67.91	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
159.8.28.242	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
159.8.28.242	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
159.8.28.242	147.237.77.74	United States	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
132.74.95.21	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
159.8.28.242	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	3
159.8.28.242	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.78.144	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
54.209.60.63	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.67.125	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
159.8.28.242	147.237.77.234	United States	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
31.168.101.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
159.8.28.242	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	2
159.8.28.242	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
159.8.28.242	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
159.8.28.242	147.237.77.216	United States	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
159.8.28.242	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
185.37.212.6	147.237.76.196	Spain	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.67.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.194	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	2
176.13.0.47	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
159.8.28.242	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
159.8.28.242	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.102.8.178	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
159.8.28.242	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	2
94.102.48.194	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
192.169.226.249	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
109.65.196.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
159.8.28.242	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.249.232.152	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4110
41.249.245.175	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3580
79.181.9.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2845
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2570
114.124.37.200	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2233
194.114.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2062
114.124.35.52	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1834
31.44.137.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1656
114.121.160.132	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1607
192.116.190.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1439
114.121.161.176	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1427
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1371
190.167.253.83	Dominican Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	998
178.214.88.189	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	960
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	923
39.250.147.187	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	802
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	783
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	763
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	736
208.54.4.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	707
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	613
37.60.46.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	604
8.37.224.246	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	530
114.121.134.59	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	508
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	496
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	447
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	394
79.182.198.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	345
212.27.185.253	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	328
62.207.60.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	324
37.237.128.122	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	323
132.254.132.1	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	321
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	318
95.86.110.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	311
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	311
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	299
80.74.124.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	287
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	286
84.94.21.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	283
213.140.59.137	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	272
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	271
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	270
82.145.216.137	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	266
2.54.133.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	262
37.26.146.142	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	258
37.238.140.113	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	257
64.223.94.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	234
70.39.185.191	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	229
79.182.174.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	228
2.54.133.44	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
114.121.161.176	Indonesia	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52425
114.124.35.52	Indonesia	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50123
114.124.37.200	Indonesia	147.237.77.216	dover.idf.il	Too Many of the Same Response Code (404) in Session from 114.124.37.200	Block	33757
114.121.160.132	Indonesia	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27195
39.250.147.187	Indonesia	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15028
46.19.85.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10368
2.54.19.86	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.19.86	Block	9137
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	8034
114.124.37.200	Indonesia	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7162
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6936
114.121.134.59	Indonesia	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5441
46.19.86.45	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.45	Block	5247
176.12.148.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4675
46.19.86.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3592
5.22.129.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3281
2.54.181.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3212
46.19.86.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3108
93.173.7.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1416
46.19.85.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1276
2.54.177.82	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.177.82	Block	1164
2.54.31.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1164
41.249.245.175	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.249.245.175	Block	1129
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.232	Block	987
176.12.137.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	843
75.126.122.176	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	792
176.13.14.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	524
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	504
212.179.195.66	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.195.66	Block	468
85.250.72.67	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 85.250.72.67	Block	384
2.52.10.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	360
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	300
41.249.245.175	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.249.245.175	Block	291
91.200.12.130	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	288
91.200.12.130	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.130	Block	276
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	276
82.166.65.241	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	239
176.13.7.183	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.7.183	Block	216
85.64.151.187	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.151.187	Block	204
46.120.23.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	192
91.200.12.63	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.63	Block	192
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	180
91.212.124.173	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	144
91.200.12.19	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	144
91.200.12.116	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	144
87.69.81.112	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	144
91.200.12.63	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	144
91.200.12.19	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.19	Block	132
46.229.164.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.102	Block	132
91.200.12.116	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.116	Block	132
79.177.4.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	132