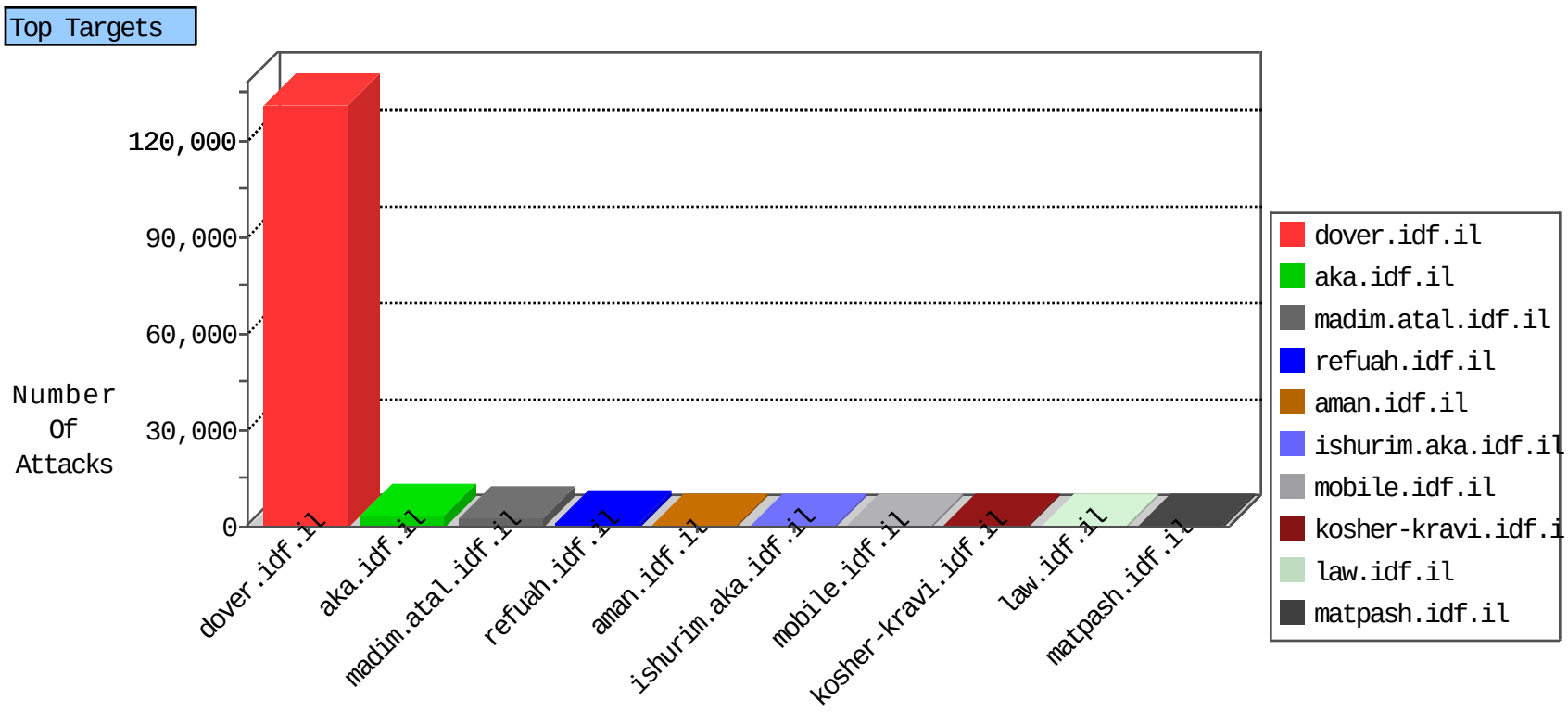
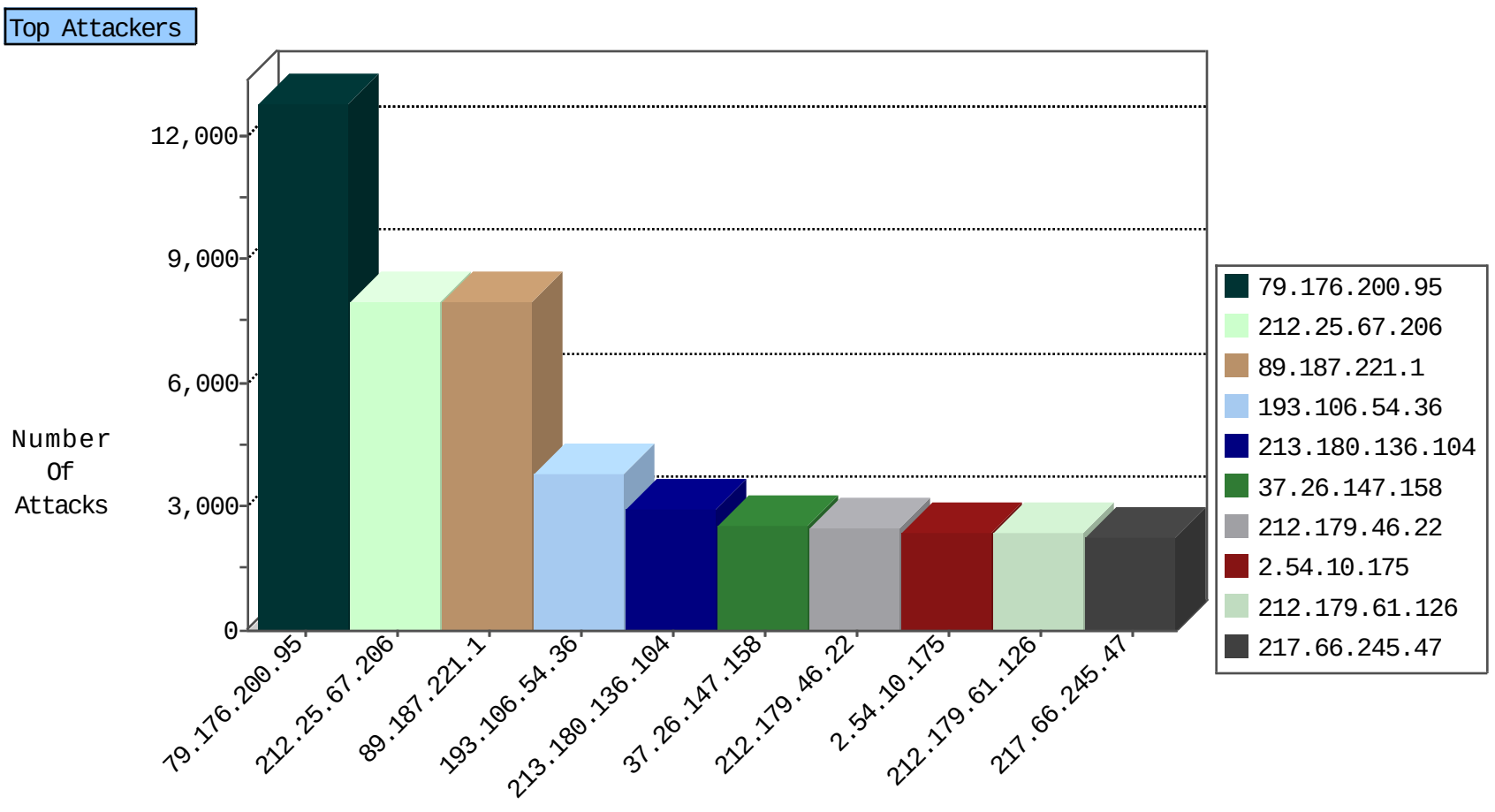
04-30-2015-00:00:03 to 05-01-2015-00:00:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-30-2015-00:00:03 to 05-01-2015-00:00:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.67.76	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5030
66.249.67.92	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4466
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4381
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3260
66.249.64.98	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2885
176.12.145.44	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2837
89.139.0.139	Israel	147.237.0.15	kosher-kravi.idf.i	TCP Scan (vertical)	drop	2726
212.25.67.206	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2707
195.160.240.11	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2602
46.19.85.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2595
66.249.67.84	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2571
212.150.203.146	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2560
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2552
212.179.46.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2552
66.249.67.116	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1185
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1131
66.249.64.2	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	989
220.181.108.82	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	761
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	461
79.180.193.228	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	366
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	366
199.119.124.41	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	344
84.109.51.168	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	298
66.249.64.64	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	294
66.249.79.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	259
84.109.235.14	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	255
46.121.238.237	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	229
84.228.161.227	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	224
220.181.108.165	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	218
212.117.140.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
66.249.78.11	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	192
93.173.136.190	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
176.228.17.77	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
220.181.108.142	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	175
168.235.195.123		147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	172
220.181.108.181	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	171
220.181.108.86	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	165
66.249.64.39	Israel	147.237.0.15	kosher-kravi.idf.i	TCP handshake violation, first packet not syn	drop	164
220.181.108.100	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	160
2.54.13.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
109.65.224.108	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	149
85.64.117.146	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	145
109.253.159.167	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
84.228.105.39	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
46.120.245.47	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
109.253.133.209	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
46.19.86.88	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
93.173.2.75	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	81

04-30-2015-00:00:03 to 05-01-2015-00:00:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.180.136.104	Poland	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2928
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	413
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	182
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	63
62.90.220.150	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	25
5.29.109.51	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	21
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
81.218.116.129	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
85.250.198.165	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	14
50.118.255.237	United States	147.237.77.233	atal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
79.180.165.198	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
2.52.23.17	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
66.240.236.119	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	9
79.183.166.188	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
46.19.85.192	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	8
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	7
84.229.30.234	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	7
79.182.63.98	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
66.240.236.119	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	7
49.151.73.29	Philippines	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
77.125.216.244	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.34.12.154	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
66.240.236.119	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	6
5.102.233.36	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.186.170.59	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
66.240.236.119	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
93.172.84.71	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	5
46.120.74.134	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.117.11.194	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	5
192.114.23.18	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.116.202.157	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	4
84.109.180.46	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
91.105.238.22	Russian Federation	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	4

04-30-2015-00:00:03 to 05-01-2015-00:00:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN Vega Web Application Scan	1084
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL Injection - Select From	105
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	105
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	100
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	93
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	93
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	93
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	93
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	93
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	93
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	93
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	93
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	93
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	93
89.139.0.139	Israel	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	31
46.19.86.211	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	15
80.246.136.137	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	14
37.239.68.72	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	9
37.239.68.195	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	8
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	GPL WEB_SERVER .htaccess access	7
217.66.245.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP .htaccess access	7
149.78.133.60	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
66.249.67.108	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.67.92	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.144	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.116	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
162.144.104.122	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.76	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
84.108.174.212	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
89.139.0.139	Israel	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	3
46.19.85.70	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
87.69.211.184	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
46.120.5.104	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.78.100.108	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.33.127.200	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.42	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	2
61.183.128.6	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
147.236.31.182	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.238.58	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.64	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
58.20.54.249	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
61.183.128.6	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
87.68.47.104	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.193.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.28.30	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
192.117.10.227	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.138.233.11	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

04-30-2015-00:00:03 to 05-01-2015-00:00:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.176.200.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12797
212.25.67.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7977
89.187.221.1	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7951
193.106.54.36	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3803
37.26.147.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2535
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2489
2.54.10.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2389
212.179.61.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2361
2.52.54.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2221
212.76.96.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2065
2.54.57.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2007
95.86.101.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1748
2.54.144.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1631
212.179.21.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1606
212.143.3.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1476
213.151.35.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1348
37.239.68.195	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1333
212.199.244.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1195
82.145.216.241	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1122
2.54.43.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	966
37.26.146.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	919
84.94.191.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	901
46.19.86.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	858
164.138.123.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	825
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	733
37.26.147.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	698
212.76.99.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	629
80.230.61.216	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	535
212.179.21.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	458
37.60.43.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	452
2.52.52.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	446
194.114.146.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	446
37.142.118.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	392
81.218.251.250	Israel	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	351
204.52.189.242	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	344
209.37.66.194	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	325
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	318
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	316
46.19.85.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	314
46.117.11.194	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	301
46.235.152.13	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	291
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	290
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	282
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	280
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	279
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	264
5.29.30.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	262
207.46.13.92	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	261
79.180.154.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	254

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.65.14.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	732
212.76.121.2	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 212.76.121.2	Block	699
46.117.58.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	302
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.84	Block	201
80.246.139.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	184
2.54.32.213	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.32.213	Block	178
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	127
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	77
176.12.137.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	74
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	71
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	66
46.19.86.144	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.144	Block	54
80.246.140.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	38
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	34
109.253.133.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	34
207.46.13.86	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.86	Block	33
80.246.138.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	31
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	31
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	30
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.128	Block	22
176.12.140.168	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.140.168	Block	21
207.46.13.19	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.19	Block	20
213.8.129.152	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	18
79.183.202.215	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	17
109.67.117.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	16
79.183.63.92	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	16
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
77.127.172.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	15
176.12.139.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
207.46.13.3	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.3	Block	13
93.172.204.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
64.187.228.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 64.187.228.146	Block	11
157.55.39.210	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.210	Block	11
37.142.234.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	10
54.88.168.129	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 54.88.168.129	Block	10
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
62.0.1.170	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	10
77.66.121.237	Denmark	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.66.121.237	Block	9
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
125.65.46.140	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 125.65.46.140	Block	8
207.46.13.114	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il//captcha.ashx	Block	8
95.86.106.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.106.185	Block	8
195.190.19.253	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	7
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
185.13.195.17	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.aspx.co.il	Block	6
95.86.127.95	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
157.55.39.146	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.146	Block	6
188.120.140.47	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	6