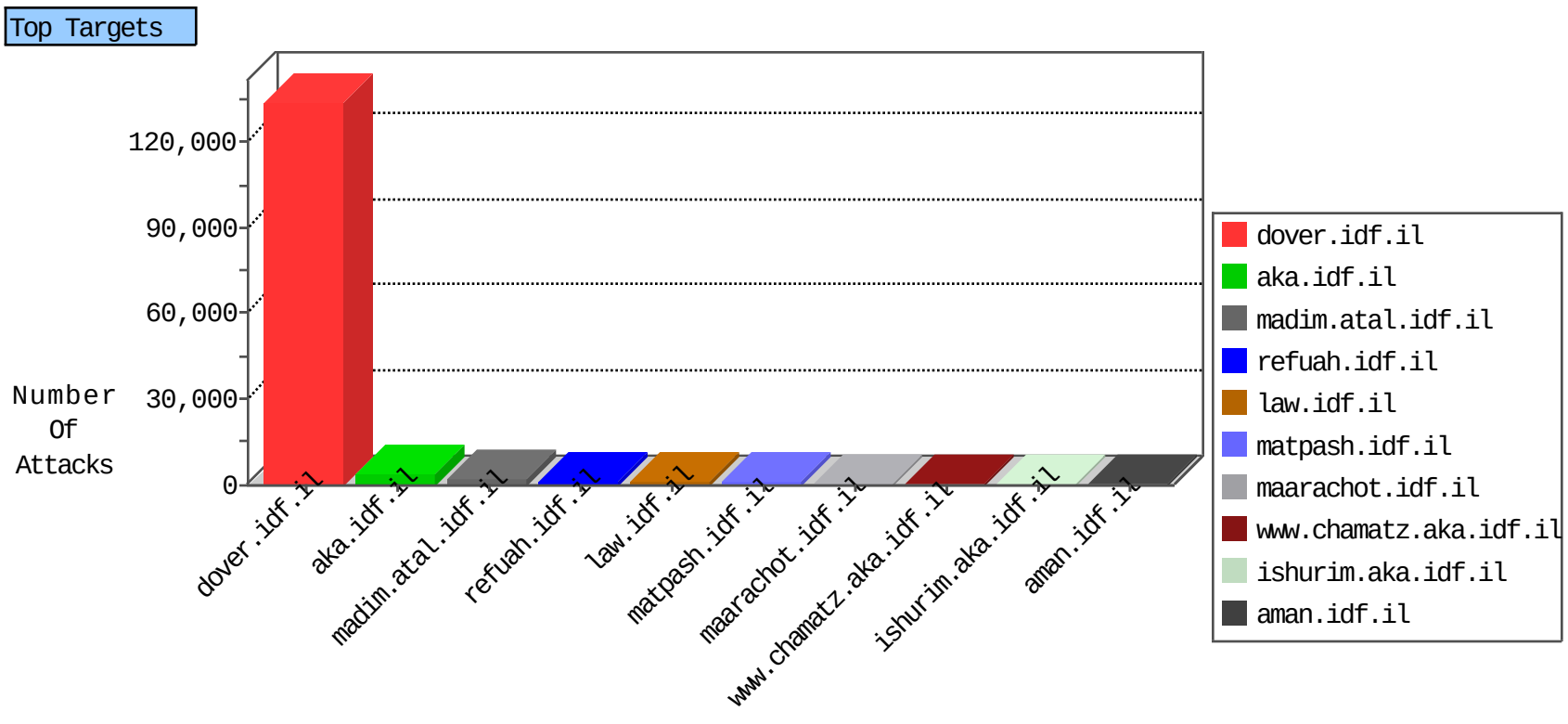
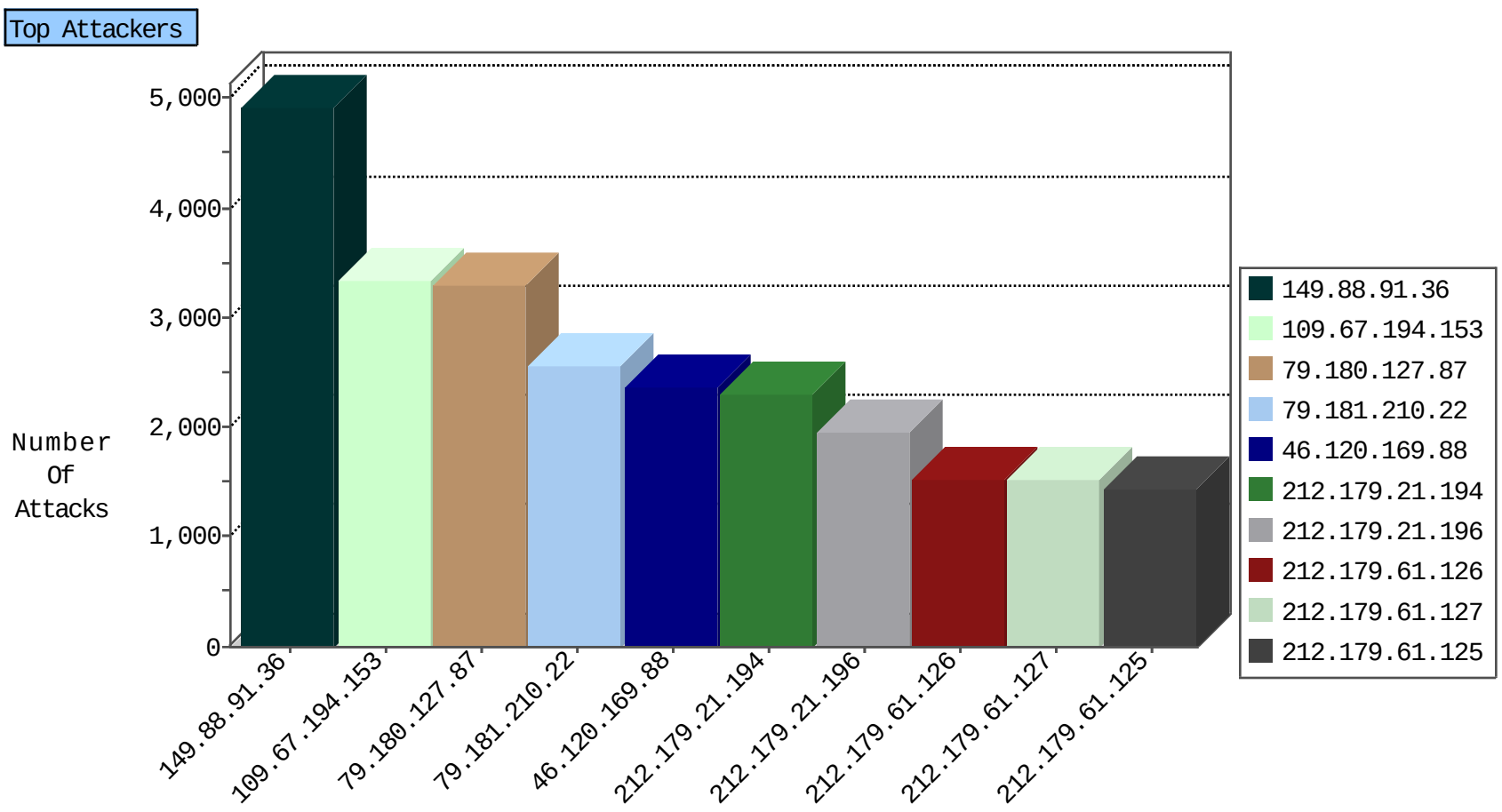
04-27-2015-00:00:09 to 04-28-2015-00:00:09

IDF Under Attack Daily Report



Top Target



Top Attackers

04-27-2015-00:00:09 to 04-28-2015-00:00:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	42774
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	37437
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	32091
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	25514
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	19901
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	8747
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	8460
66.249.78.11	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7700
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5842
220.181.108.115	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	5493
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4403
66.249.78.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	4073
220.181.108.139	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	4016
66.249.78.38	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	3291
79.176.52.30	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3009
66.249.64.64	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3003
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2742
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2713
79.183.0.96	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2574
66.249.78.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2529
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2164
94.159.222.105	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1769
201.58.130.165	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1337
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1320
87.68.152.111	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1203
66.249.64.98	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	971
109.64.232.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	965
66.249.78.76	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	819
66.249.64.66	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	670
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	655
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	581
66.249.64.2	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	558
220.181.108.115	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	504
66.249.75.117	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	485
157.55.39.58	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	457
31.168.126.160	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	427
220.181.108.139	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	407
220.181.108.142	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	403
220.181.108.120	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	399
87.68.165.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	392
220.181.108.109	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	391
46.120.34.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	384
220.181.108.184	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	383
212.179.21.198	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	361
192.114.182.2	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	349
5.102.226.18	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	325
31.168.103.115	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	298
66.249.64.4	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	295
220.181.108.153	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	295
66.249.78.62	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	289

04-27-2015-00:00:09 to 04-28-2015-00:00:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	261
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	256
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	207
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	168
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	165
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	104
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	90
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	46
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	41
107.183.220.254	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
199.168.141.77	United States	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	35
117.131.78.26	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	34
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
60.10.71.107	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	17
146.148.47.140		147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
104.155.28.201		147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
146.148.47.140		147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
104.155.28.201		147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
23.251.55.233	United States	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
194.114.146.227	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
66.240.236.119	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	7
84.228.175.229	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
66.240.236.119	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	7
94.230.86.214	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
82.80.17.163	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
37.46.41.84	Israel	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	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	6
212.179.155.129	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.176.158.131	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	6
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	6
91.135.111.75	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
66.240.236.119	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	6
87.68.145.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
66.240.236.119	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	6
66.240.236.119	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	6
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	5
137.54.8.77	United States	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	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	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	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	5

04-27-2015-00:00:09 to 04-28-2015-00:00:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	394
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	90
84.228.227.69	Israel	147.237.76.86	navy.idf.il	GPL SCAN nmap TCP	32
41.193.5.57	South Africa	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	28
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	10
2.54.133.152	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
178.216.51.2	Sweden	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	5
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	5
176.12.146.157	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
213.165.69.91	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.69.77	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
41.42.45.79	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP JBoss JMX console access attempt	4
41.42.45.79	Egypt	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	4
41.42.45.79	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	4
66.249.64.2	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
128.199.118.86	Singapore	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
41.42.45.79	Egypt	147.237.77.216	dover.idf.il	ET WEB_SPECIFIC_APPS Possible JBoss JMX Console Beanshell Deployer WAR Upload and Deployment Exploit Attempt	3
189.3.154.195	Brazil	147.237.0.16	my-kosher-kravi.idf.il	GPL SCAN nmap TCP	3
94.73.165.106	Turkey	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
205.234.138.122	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
185.32.178.111	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
79.183.59.203	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.150.189.2	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
189.3.154.195	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	GPL SCAN nmap TCP	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
5.29.222.21	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.2.204.134	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.120.200.30	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.14.206	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.75.117	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.161	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
5.29.17.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.12.142	Israel	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
213.57.182.163	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
81.218.77.162	Israel	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
66.249.67.92	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
109.186.164.109	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
58.20.54.249	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	2
84.111.141.32	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.22.130.2	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
81.218.77.162	Israel	147.237.0.34	tikshuv.idf.il	GPL SCAN nmap TCP	2
66.249.64.78	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
87.68.148.150	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
61.240.144.65	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2

04-27-2015-00:00:09 to 04-28-2015-00:00:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
149.88.91.36	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4925
109.67.194.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3334
79.180.127.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3303
79.181.210.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2564
46.120.169.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2375
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2265
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1959
212.179.61.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1519
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1480
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1431
85.250.68.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1304
109.64.190.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1280
79.183.66.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1252
77.125.24.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1240
79.182.219.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1100
2.52.188.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1036
46.19.85.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1029
46.120.72.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	914
108.58.22.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	896
46.19.86.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	888
176.12.146.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	800
95.86.116.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	754
89.139.174.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	739
94.159.215.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	713
95.86.125.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	692
109.64.142.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	619
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	587
46.19.85.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	575
80.230.93.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	574
46.117.108.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	570
79.180.137.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	564
149.78.103.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	554
192.116.128.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	541
77.125.33.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	538
81.218.123.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	508
176.12.145.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	484
66.249.78.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	475
82.145.210.29	Europe	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	462
2.54.175.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	460
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	459
79.179.30.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	452
66.249.78.109	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	450
109.64.99.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	444
62.128.35.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	440
37.26.147.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	437
66.249.78.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	437
66.249.78.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	426
66.249.78.102	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	426
92.74.228.69	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	424
66.249.69.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	418

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.158.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	438
46.120.152.40	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.120.152.40	Block	362
2.54.157.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	308
2.54.185.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	271
2.54.154.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	247
2.52.23.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	105
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	96
109.253.157.220	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.157.220	Block	59
85.65.247.48	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 85.65.247.48	Block	44
46.19.85.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	42
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	39
77.127.214.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	30
176.12.148.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	29
142.54.165.154	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 142.54.165.154	Block	28
99.103.210.40	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	26
77.126.225.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	19
46.19.85.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	18
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	16
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.58	Block	14
176.12.146.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	13
213.8.52.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	13
2.54.141.157	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.141.157	Block	13
79.183.58.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	12
94.159.162.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	12
176.228.178.232	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.228.178.232	Block	12
176.12.146.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
176.12.151.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	11
46.121.218.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
80.246.133.229	Israel	147.237.76.31	nakchal.idf.il	Distributed Suspicious Response Code	Block	11
66.249.75.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.74	Block	10
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
212.179.132.202	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	9
87.69.241.92	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 87.69.241.92	Block	9
81.218.46.66	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
149.78.82.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	8
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.48	Block	8
60.10.71.107	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 60.10.71.107	Block	8
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	8
79.179.13.103	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
80.178.251.210	Israel	147.237.76.86	navy.idf.il	Too Many of the Same Response Code (404) in Session from 80.178.251.210	Block	8
149.88.85.237	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
207.46.13.52	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.52	Block	7
41.42.45.79	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.42.45.79	Block	7
79.183.138.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
31.44.141.68	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
176.12.147.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	7
66.249.75.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.66	Block	7
2.52.23.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	7