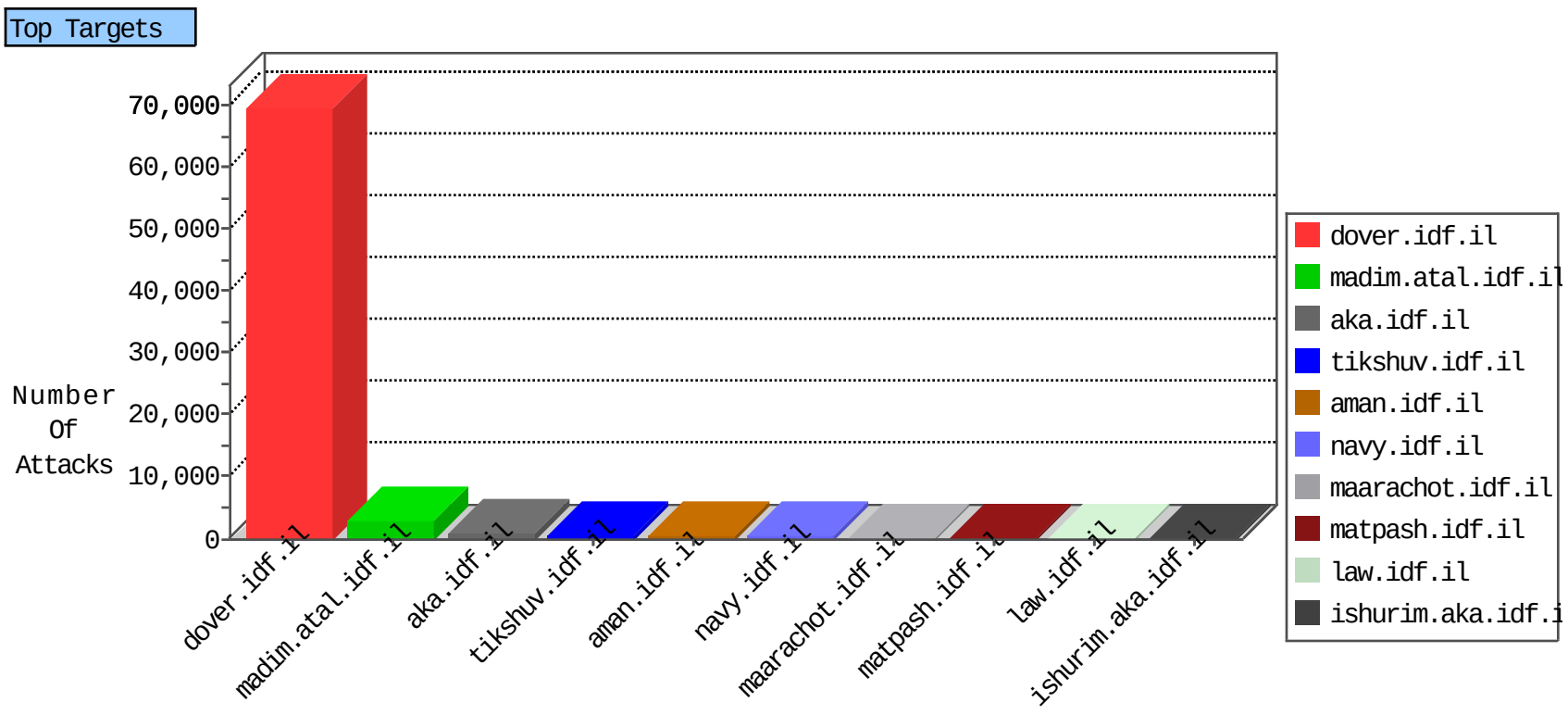
04-23-2015-00:00:04 to 04-24-2015-00:00:04

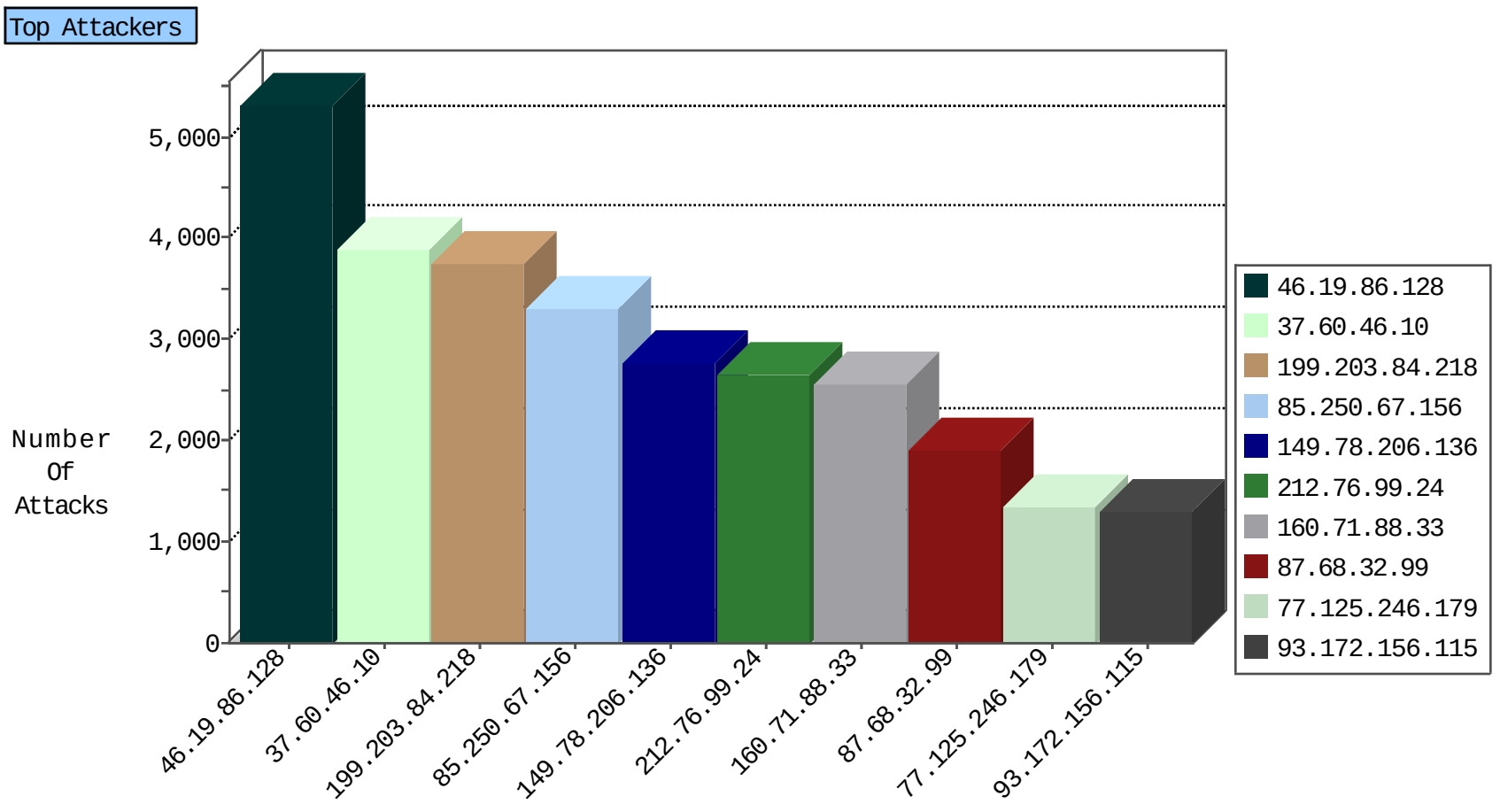
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-23-2015-00:00:04 to 04-24-2015-00:00:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	17108
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	11619
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	9392
46.19.85.57	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3686
68.198.155.187	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3294
79.177.58.230	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3263
82.80.61.143	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3208
77.125.160.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3083
208.104.107.186	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2895
137.135.176.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2853
220.181.108.150	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	2619
85.210.34.175	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2537
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2474
84.111.108.97	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1258
77.126.40.68	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1199
160.71.88.33	Finland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1013
46.120.184.231	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	964
79.178.143.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	876
139.74.160.22	Finland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	834
79.177.133.134	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	819
84.108.63.47	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	814
62.218.31.10	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	787
220.181.108.103	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	744
108.41.12.139	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	622
46.116.106.38	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	567
77.126.68.27	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	537
87.68.48.118	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	525
109.66.10.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	496
220.181.108.118	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	479
220.181.108.90	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	467
220.181.108.112	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	456
220.181.108.100	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	437
79.178.190.28	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	407
220.181.108.186	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	389
220.181.108.171	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	371
94.123.152.100	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	357
77.127.241.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	342
66.249.78.25	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	330
80.179.163.218	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	307
85.250.100.35	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	280
84.108.110.139	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	249
80.246.130.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	246
66.249.78.11	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	237
2.54.23.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	235
84.108.240.237	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	231
79.183.101.38	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	224
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	223
109.70.165.114	Finland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	206
93.173.136.90	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	175
87.69.247.225	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	172

04-23-2015-00:00:04 to 04-24-2015-00:00:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
87.68.32.99	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1910
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	99
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	94
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	63
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	39
195.93.60.35	Germany	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	38
104.149.17.176		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	35
198.15.178.4	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	28
198.204.243.117	United States	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	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
198.204.243.117	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	16
130.211.187.65		147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
130.211.187.65		147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
95.15.171.67	Turkey	147.237.72.166	aka.idf.il	12373: HTTP: WordPress admin Login	Block	8
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	7
79.182.205.26	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
104.33.143.209		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
113.210.3.127	Malaysia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
198.20.70.114	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	6
178.214.66.49	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.117.250.156	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.146	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.116.107.100	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.165	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.182.218.82	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.111.240.76	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.55	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.162	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.25.103.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
109.65.16.193	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.34	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.172	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
129.194.252.40	Switzerland	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.236	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	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
71.6.167.142	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.156	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.192.138	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	4
85.65.165.29	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.138	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4

04-23-2015-00:00:04 to 04-24-2015-00:00:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	127
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	125
66.249.81.206	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	60
109.65.58.254	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	32
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	16
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	16
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	12
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	12
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	10
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	5
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.14	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.73.219	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.44	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
85.102.18.198	Turkey	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	3
132.74.95.21	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
85.104.247.246	Turkey	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	3
122.228.207.76	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
213.41.72.13	France	147.237.77.176	matpash.idf.il	GPL SCAN nmap TCP	2
79.180.12.182	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.76.96.241	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.41.155	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
132.64.33.249	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
58.20.54.249	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
210.21.70.180	China	147.237.77.205	prisha.idf.il	GPL SCAN nmap TCP	2
122.228.207.77	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
46.117.110.252	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.11	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
109.65.134.14	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.136.29	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
46.19.86.168	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.250.194.159	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.86.21	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.250.78.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
193.107.17.72	Russian Federation	147.237.77.170	maarachot.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
66.249.65.46	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
122.228.207.76	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.160	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.147	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.65.39	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
5.22.129.174	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
122.228.207.76	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.154	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
85.65.213.23	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

04-23-2015-00:00:04 to 04-24-2015-00:00:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.128	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5325
37.60.46.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3896
199.203.84.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3747
85.250.67.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3308
149.78.206.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2766
212.76.99.24	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2650
160.71.88.33	Finland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2550
77.125.246.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1348
93.172.156.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1282
2.54.185.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	849
85.64.178.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	808
84.228.243.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	788
77.127.221.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	783
95.86.75.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	760
95.86.73.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	700
85.64.84.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	649
2.54.152.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	595
2.54.151.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	564
2.54.191.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	487
2.54.187.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	446
89.138.64.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	427
2.54.169.0	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	370
109.64.11.47	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	367
2.54.62.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	350
212.76.96.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	326
77.126.20.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	300
95.86.68.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	300
5.29.169.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	297
87.68.250.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	280
46.117.164.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	262
188.64.102.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	250
80.178.235.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	250
84.228.181.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	242
212.179.21.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	216
217.9.101.140	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	200
2.54.10.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	200
50.118.172.30	United States	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	200
216.177.129.150	United States	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	188
46.19.86.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	181
80.230.109.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	180
93.173.177.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	179
89.187.221.1	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	178
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	177
46.116.223.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	171
95.86.111.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	162
176.58.108.28	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	151
95.86.114.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	150
69.237.149.11	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	150
77.125.74.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	117
109.65.196.99	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	116

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.65.165.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	695
79.177.13.246	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.177.13.246	Block	450
109.186.173.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	305
46.19.86.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	267
80.246.136.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	194
185.32.178.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	165
80.246.140.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	160
176.12.144.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	138
176.12.140.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	119
93.172.23.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	118
2.54.31.7	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.31.7	Block	72
89.139.45.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	62
176.12.142.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
84.228.13.81	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	55
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	41
84.109.107.194	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	36
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	29
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
87.69.92.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
176.12.150.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	24
2.54.158.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	22
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	22
176.12.136.231	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.136.231	Block	20
125.65.81.124	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 125.65.81.124	Block	20
82.173.165.123	Netherlands	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.173.165.123	Block	18
84.109.105.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	18
84.229.66.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	17
93.172.31.139	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 93.172.31.139	Block	14
84.108.61.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
46.120.161.229	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
37.46.39.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	12
79.180.12.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	11
87.69.128.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	11
79.183.145.162	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.183.145.162	Block	9
109.66.22.188	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
2.54.1.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	9
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	9
109.66.5.244	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	8
87.69.78.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
109.186.49.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
80.246.138.86	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 80.246.138.86	Block	7
149.88.8.108	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
149.78.46.42	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 149.78.46.42	Block	7
37.139.52.23	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	6
84.94.41.205	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	6
46.116.106.145	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.116.106.145	Block	6
37.26.146.179	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
79.178.4.108	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
79.177.9.224	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6